AFCRL-71-0013

ALGEBRAIC THEORY OF CODES II

Edward F. Assmus, Jr.
Harold F. Mattson, Jr.

GTE SYLVANIA
INCORPORATED
ELECTRONIC SYSTEMS GROUP
EASTERN DIVISION

77 "A" STREET
NEEDHAM HEIGHTS, MASSACHUSETTS 02194

Contract No. F19628-69-C-0068
Project No. 5628
Task No. 562801
Work Unit No. 56280101

FINAL REPORT

Period Covered: 16 September 1969 - 15 September 1970

15 October 1970

Contract Monitor: Vera S. Pless
Data Sciences Laboratory

This document has been approved for public release and sale; its distribution is unlimited.

Prepared for

AIR FORCE CAMBRIDGE RESEARCH LABORATORIES
AIR FORCE SYSTEMS COMMAND
UNITED STATES AIR FORCE
BEDFORD, MASSACHUSETTS 01730

68

AFCRL-71-0013

ALGEBRAIC THEORY OF CODES II

Edward F. Assmus, Jr.
Harold F. Mattson, Jr.

GTE SYLVANIA
INCORPORATED
ELECTRONIC SYSTEMS GROUP
EASTERN DIVISION

77 "A" STREET
NEEDHAM HEIGHTS, MASSACHUSETTS 02194

Contract No. F19628-69-C-0068
Project No. 5628
Task No. 562801
Work Unit No. 56280101

FINAL REPORT

Period Covered: 16 September 1969 - 15 September 1970

15 October 1970

Contract Monitor: Vera S. Pless
Data Sciences Laboratory

This document has been approved for public release and sale; its distribution is unlimited.

Prepared for

AIR FORCE CAMBRIDGE RESEARCH LABORATORIES
AIR FORCE SYSTEMS COMMAND
UNITED STATES AIR FORCE
BEDFORD, MASSACHUSETTS 01730

ABSTRACT

The resultant is applied to the problem of weights in cyclic codes. The binary code arising from the projective plane of order 10 (if it exists) is examined. T-design decoding is discussed in general. and the special case of the (48, 24) binary extended quadratic residue code is worked out in detail. The (60, 30) ternary extended quadratic residue code is proved to yield new 5-designs. Miscellaneous results include study of the question whether Steiner triple systems support linear codes.

TABLE OF CONTENTS

PART I

A RESULTANT APPROACH TO CYCLIC CODES

We begin with an elementary remark on weights occurring in some cyclic codes. Let n be prime and consider a cyclic code of length n over $GF(q) = F$. Let ζ be a primitive n-th root of 1. Then $K = F(\zeta)$ is a field of degree $[K:F]$ = the multiplicative order of q modulo n. Let us suppose $[K:F] = e\phi$ and let L be the intermediate field as indicated:

$$\begin{tikzcd}
K \arrow[d, dash, "\phi"] \\
L \arrow[d, dash, "e"] \\
F
\end{tikzcd}$$

The i-th coordinate of a vector in the cyclic code is expressed as:

$$T\left(c_1\zeta^{e_1 i}\right) + T\left(c_2\zeta^{e_2 i}\right) + \ldots + T\left(c_r\zeta^{e_r i}\right)$$

where the $e_1, \ldots, e_r$ are in different orbits under multiplication by $1, q, \ldots, q^{e\phi-1}$ in the integers mod n. This means that there is the usual polynomial f(x), depending on $c_1, \ldots, c_r$, such that the degree of f(x) is less than n and its coefficients are in K, and the i-th coordinate of the corresponding code-vector is $f\left(\zeta^i\right)$. f(x) is the formal trace $T\left(c_1x^{e_1} + \ldots + c_rx^{e_r}\right)$ with exponents on x reduced mod n.

The number of 0's in the code-vector is the degree of the greatest common divisor (g.c.d.) $\left(x^n-1, f(x)\right)$.

Now suppose we restrict the $c_1, \ldots, c_r$ to lie in L. Then f(x) has coefficients in L; and, therefore, the g.c.d. must consist of some divisor of x^n-1 over L. Under our assumptions, x^n-1 factors into x-1 and a number of other irreducible polynomials all of degree ϕ. Therefore, the g.c.d. has degree $\lambda\phi$ or $\lambda\phi + 1$. In other words, when the $c_1, \ldots, c_r$ are in L, the weight of the corresponding code-vector is congruent mod ϕ to n or n-1.

We can determine which of these possibilities arises to an extent. Let $q = p^s$ for a prime p.

Case 1. p divides ϕ. Then $f(1) = 0$ as $T_{K/F}(c) = \phi T_{L/F}(c)$ for $c \in L$. Thus, x-1 always divides the g.c.d., so here the weights are n-1 mod ϕ.

Case 2. p does not divide δ. Then both cases arise because there are always c in L with "small" trace 0 and non-0, respectively.

This completes our first remark, and we now analyze the g.c.d. more carefully and in general, by means of some elementary and very classical algebra.

The greatest common divisor $g(x)$ of the polynomials $f(x)$ and $h(x)$ over the field F is defined as the monic polynomial over F of highest degree dividing both $f(x)$ and $h(x)$. Unless $f(x) = h(x) = 0$, it is unique; and it exists as the polynomial of lowest degree among those of the form $r(x)\ f(x) + s(x)\ h(x)$ as $r(x)$ and $s(x)$ run over $F[x]$. This characterization of the g.c.d. shows that it remains unchanged if the field F is extended. These facts follow immediately from the Euclidean algorithm. The following additional properties hold:

$$\text{Let } r(x)\ f(x) + s(x)\ h(x) = g(x). \tag{1}$$

with the notation as above. On dividing by $g(x)$, we see that $r(x)$ and $s(x)$ are relatively prime. Also, there exist $r(x)$ and $s(x)$ satisfying (1) such that

$$\deg r(x) < \deg h(x) \text{ and } \deg s(x) < \deg f(x) \tag{2}$$

One proves (2) easily with the Euclidean algorithm. Using (2) and dividing (1) by $g(x)$, one sees that we can choose $r(x)$ and $s(x)$ in (1) so that

$$\begin{aligned} &\deg r(x) < \deg h(x) - \deg g(x) \\ &\deg s(x) < \deg f(x) - \deg g(x) \end{aligned} \tag{3}$$

Suppose now we are given the polynomials $f(x)$ and $h(x)$ explicitly as

$$f(x) = a_0 x^m + a_1 x^{m-1} + \ldots + a_m$$

$$h(x) = b_0 x^n + b_1 x^{n-1} + \ldots + b_n$$

Using (2) we could then set up $m + n$ linear equations for the unknown coefficients of $r(x)$ and $s(x)$, with the right-hand side being the unknown coefficients of $g(x)$. If we ordered the equations just so, we would have for the (square) matrix M of coefficients (of size $m + n$)

$$\begin{array}{l}
\left.\begin{array}{cccccccc}
a_o & a_1 & \cdots & a_m & 0 & \cdots & 0 \\
0 & a_o & a_1 & \cdots & a_m & 0\ldots 0 & \\
 & & \vdots & & \vdots & & \\
0 & 0 & \cdots & 0 & a_o & a_1\ldots a_m &
\end{array}\right\}\ \text{n rows} \\
\left.\begin{array}{cccccccc}
0 & 0 & \cdots 0 & b_o & b_1 & \cdots & b_n \\
0 & 0 & \cdots b_o & b_1 & \cdots & b_n & 0 \\
 & & \iddots & & & & \\
b_o & b_1 \cdots & & b_n & 0 & \cdots & 0
\end{array}\right\}\ \text{m rows}
\end{array} \tag{4}$$

Then for arbitrary polynomials r(x) and s(x) of degrees less than n and m, respectively, the coefficients of a polynomial of the form $r(x)\ f(x) + s(x)\ h(x)$ arise as

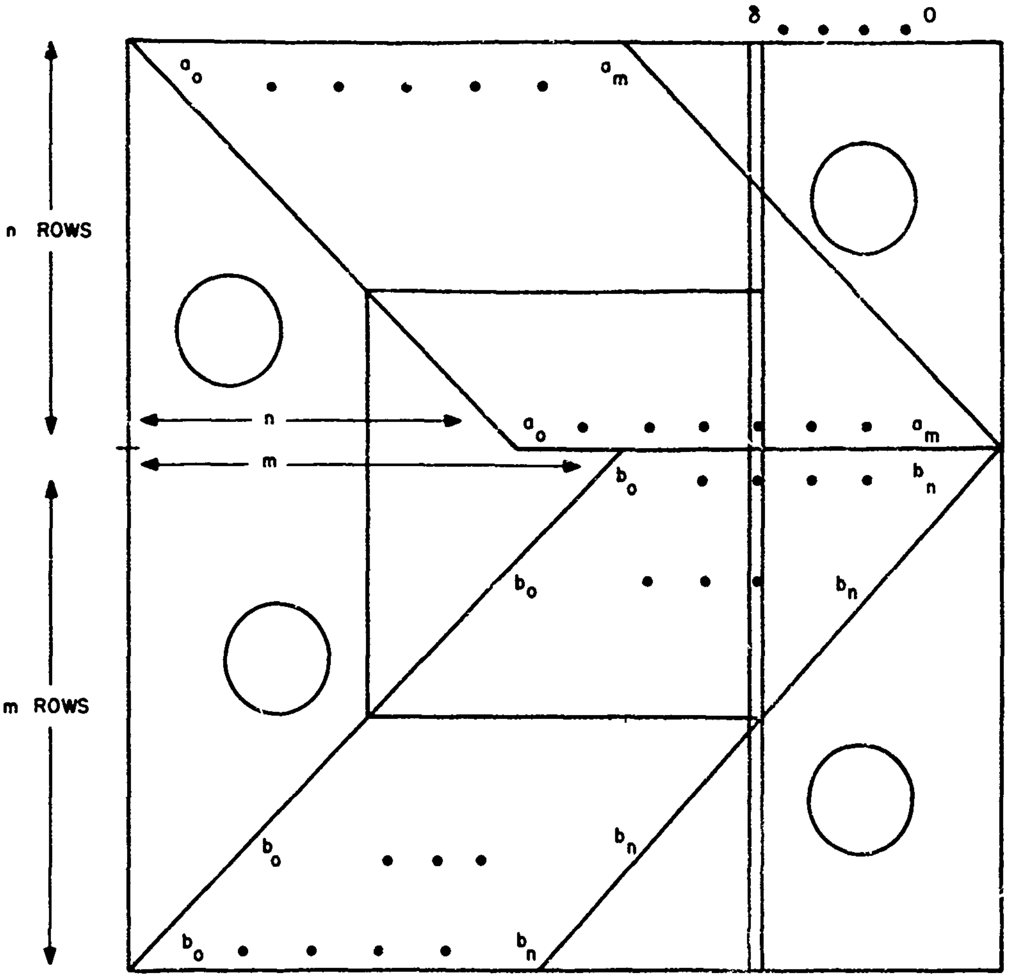
$$\Big(\underset{\text{hi}}{\cdots}\ r_i \underset{\text{lo}}{\cdots}\ ;\quad \underset{\text{lo}}{\cdots}\ s_j \underset{\text{hi}}{\cdots}\Big)M = \Big(\underset{\text{hi}}{\ }\cdots\underset{\text{lo}}{\ }\Big) \tag{5}$$

in an obvious notation for the polynomial coefficients as row-vectors.

The degree of g(x). Number the columns of M from the right, starting with 0. Suppose the δ-th column has the property that it and the columns to the left of it span all the columns of M, and that this is the left-most such column. The δ is the degree of the g.c.d. g(x). When $\delta = 0$, M is non-singular and $g(x) = 1$.

The reason for this is that a non-0 set of coefficients r_i and s_i on the left of (5) can be chosen to annihilate all columns to the left of the δ-th, but not the δ-th column. This choice yields the maximum string of consecutive 0's on the high-degree end of the right-hand side of (5) without producing all 0's there. (Incidentally, this shows the uniqueness, up to a constant factor, of r(x) and s(x) in (1), satisfying (2), because the annihilator of the subspace of columns of co-dimension 1 has dimension 1.)

We now look at the foregoing in terms of the matrix M. (This is adapted from [2] and apparently goes back at least to Bôcher [1], when it was all probably very standard.) Suppose the δ-th column is defined as above and that we consider the small matrix M_δ (of $m + n - 2\delta$ rows and columns) obtained by peeling off δ columns from each side and δ rows from top and bottom of M. Because we know there are r(x) of degree at most $n-\delta$ and s(x) of degree at most m-δ satisfying (1), we know that the columns of M_δ are linearly independent. Therefore, det $M_\delta \neq 0$.



If, however, we expand M_δ to M_j by removing only j rows top and bottom and on each side, with j < δ, then det M_j = 0 simply becasue the δ-th column and those to the left of it span all the columns. We have proved:

LEMMA. The largest "central" submatrix of M which is non-singular has m + n - 2δ rows and columns, where δ is the degree of the g.c.d. of f(x) and h(x).

We now apply this result to coding theory. It really provides a general way to restate the minimum-distance problem for cyclic codes.

In the general cyclic code the code-vectors $\left(a_0, \ldots, a_{n-1}\right)$ are given as $\left(f(1), f(\zeta), \ldots, f\left(\zeta^{n-1}\right)\right)$, ζ being a primitive n-th root of 1 over GF(q) = F. The polynomial f(x) is essentially a sum of traces from $K = F(\zeta) = GF\left(q^u\right)$ to F, namely

$$f(x) = T\left(c_1 x^{e_1} + c_2 x^{e_2} + \ldots + c_r x^{e_r}\right), \quad c_1, \ldots, c_r \epsilon K \tag{6}$$

where by $T\left(cx^e\right)$, we mean $cx^e + c^q x^{(qe)} + c^{q^2} x^{\left(q^2 e\right)} + \ldots + c^{q^{s-1}} x^{\left(q^{s-1} e\right)}$, where $\left(q^i e\right)$ means (here only) the least positive residue of $q^i e$ mod n. f(x) depends on $c_1, \ldots, c_r$. The code-vector corresponding to $c_1, \ldots, c_r$, has weight n-δ, where δ is the number of roots of f(x) (counted without multiplicity) among 1, $\zeta, \ldots, \zeta^{n-1}$; that is, the weight of the code-vector is n-δ, where δ is the degree of g.c.d. $\left(x^n-1, f(x)\right)$. This remark characterizes, <u>in principle,</u> the weights in the cyclic code as n-δ, where δ takes the values, for the various $c_1, \ldots, c_r$, for which M_δ is the largest non-singular "central" submatrix of M. In principle, we have the several determinants det M, det M_1, det M_2, ... as polynomials in $c_1, \ldots, c_r$. Some of these polynomials vanish identically as functions on K × ... × K and some do not. The latter correspond to the weights of the code-vectors, subject to our Lemma.

We can simplify the matrix (4) in this cyclic code case by adding columns so as to eliminate the -1's in the bottom m rows, noting that $h(x) = x^n - 1$. Then we have the circulant

$$M' = \begin{array}{lcccccl}
 & & \text{n-m-1 zeros} & & & & \\
a_m & 0 & \cdot\ \cdot\ \cdot & 0 & a_0 & a_1 \cdots & a_{m-1} \\
a_{m-1} & & & & 0 & a_0 \cdots & a_{m-2} \\
a_{m-2} & & & & & 0 \cdots & a_{m-3} \\
\vdots & & & & & & \vdots \\
 & & & & & & a_0 \\
a_0 & & & & & & 0 \\
0 & & & & & & \vdots \\
\vdots & & & & & & 0 \\
0 \cdots & & 0\ a_0 & & \cdots & & a_m
\end{array}$$

as the upper right-hand n by n matrix in M as modified. The lower m rows of the modified M may be neglected now because they are

$$\begin{array}{c|ccccc|}
 & & & m & & n \\ \hline
 & & & & 1 & \\
 & 0 & & & & \\
m & & \cdot & 1 & & 0 \\
 & & \cdot & & & \\
 & 1 & & 0 & & \\ \hline
\end{array}$$

The question now becomes: for which values of the a_j's are the matrices obtained by removing the top δ rows and the right-hand δ columns from M' non-singular? We rotate M' through 90 degrees to put it in the form

$$M'' = \begin{array}{cccccc}
0 & \cdot\ \cdot\ \cdot & 0 & a_0 & a_1\ \cdot\ \cdot\ \cdot & a_m \\
 & & & & & 0 \\
\vdots & & & & & \vdots \\
0 & & & & & 0 \\
a_0 & & & & & a_0 \\
a_1 & & & & & \\
\vdots & & & & & \vdots \\
a_m & & 0\ \cdot\ \cdot\ \cdot & 0\ a_0 & & a_{m-1}
\end{array}$$

which is constant along diagonals perpendicular to the main diagonal. Such a matrix is called persymmetric. The result on weights now takes the following form.

PROPOSITION. With the a_i's in the form given by (6), the weight w occurs in the code if and only if for some choice of the a_i's, the submatrix of M'' consisting of the first w rows and columns is non-singular and every larger such submatrix is (for the same a_i's) singular.

Here we must point out the existence of the paper [3] on persymmetric matrices. Although it is largely concerned with how many persymmetric matrices there are of various types, there is a singularity criterion which amounts to a reduction to a smaller persymmetric matrix. Despite strenuous efforts, however, we were not able to use this criterion in a satisfactory way. Even on the (7, 3) binary cyclic code this method seemed difficult. A reader interested in pursuing this approach, however, might well want to examine this paper, for some modification of Daykin's methods might yield results more appropriate to this problem than those we were able to draw from it.

We did use Daykin's reduction method to prove the known result that in the (31, 10) cyclic code (with primitive 31st roots of unity ζ and ζ^5 as roots of the recursion polynomial), there are only the three weights 12, 16, and 20; and at the same time we calculated the weight distribution. This required considerable effort, however, and in trying the method for some codes over three and four symbols, and larger binary codes, we were forced to give up.

Working directly from the Proposition, however, we give simple proofs of the weight properties of the maximal-length code and of the BCH bound for cyclic codes.

The general BCH bound for cyclic codes may be stated as follows. In (6), choose r so that the degree of $x^r f(x)$, when reduced modulo x^n-1, is minimum, say m. Then the BCH lower bound on the weight in the code is n-m. The proof using our Proposition is that for $w < n-m$, the upper left-hand w × w submatrix in M'' is singular for all choices of the a_i's.

For the binary maximal-length code, $x^{-1}f(x) = \sum_{0}^{k-1} C^{2^i} x^{2^i-1}$, for $n = 2^k-1$. The rows of the circulant matrix M'' can then be represented as the polynomials r(x), xr(x), ..., $x^{2^k-2} r(x)$, where the top row is $r(x) = x^{-1}f(x)$,

$$C^{2^{k-1}} x^{2^{k-1}-1} + \dots + C = r(x)$$

and $x^i r(x)$ is reduced mod x^n-1. Now, numbering the rows 0, 1, 2, 3 ..., let us multiply the 0th, or top row, by 1, the 1st row by C, and the 2nd by C^2, the 4th by C^4, and in general, the 2^ith row by C^{2^i} for i = 0, 1, ..., k-1. We now add these chosen rows to find

$$= \frac{1}{x}(f(x) + Cxf(x) + C^2 x^2 f(x) + C^4 x^4 f(x) + \dots + C^{2^{k-1}} x^{2^{k-1}} f(x))$$

$$= \frac{1}{x}(f(x) + f(x)^2)$$

$$= \frac{1}{x}(Cx + C^{2^k} x^{2^k})$$

$$= \frac{1}{x}(Cx + Cx) = 0 \pmod{x^{2^k-1}-1}.$$

This shows not only that M'' is singular but also that every upper left-hand square submatrix after that of size 2^{k-1} is singular (since the last row involved in the linear combination is that numbered 2^{k-1}). Therefore, the only non-0 weight is 2^{k-1}.

References

[1] Maxime Bôcher, Introduction to Higher Algebra, MacMillan, New York; 1907.

[2] M.P. Epstein, "The Use of Resultants to Locate Extreme Values of Polynomials," SIAM J. Appl. Math., Vol. 16, pp. 62-70; 1968.

[3] David E. Daykin, "Distribution of Bordered Persymmetric Matrices in a Finite Field," J. Reine Angew. Math. 203 (1960), 47-54.

PART II

ON THE POSSIBILITY OF A PROJECTIVE PLANE OF ORDER TEN

We report here on work in progress since September 1969, a report of which was given at Oberwolfach, Germany at the conference "Combinatorial Aspects of Finite Geometries," March 30 – April 4, 1970.

1. Self-Orthogonal Designs.

Let $(S, \mathscr{D})$ be a t-design with $|S| = v$ and $|D| = k$ for D in $\mathscr{D}$. Thus, every t-subset of S is contained in precisely λ members of $\mathscr{D}$, where λ is some fixed integer. We say that $(S, \mathscr{D})$ is self-orthogonal if $|D \cap E|$ is even for every D and E in $\mathscr{D}$. In particular, then, we find that k is even by taking $D = E$.

Next, we determine all possible self-orthogonal designs with $\lambda = 1$; i.e., all possible self-orthogonal Steiner systems. Let $(S, \mathscr{D})$ be such a system. For $t = 1$, $\mathscr{D}$ is simply a partition of S, and whenever $v = |S|$ is even, there is precisely (up to isomorphism) one such design for every factorization

$$v = km$$

with k even. We discard this trivial case and assume $t > 1$. For $D_0 \in \mathscr{D}$ set

$$N_{t-1} = |\{D \in \mathscr{D};\ |D \cap D_0| = t-1\}|$$

An easy counting argument shows that

$$N_{t-1} = \binom{k}{t-1}\left[\frac{v-t+1}{k-t+1} - 1\right]$$

or

$$N_{t-1} = \binom{k}{t-1}\frac{v-k}{k-t+1}$$

For t even, N_{t-1} is necessarily 0 and this case cannot, obviously, occur unless $v = k$ – an even more trivial possibility which we again discard. So, we may now assume that t is odd and $t \geq 3$. If $t > 3$ we can, by contraction, reduce to a self-orthogonal design with $t = 3$; having determined these, all other self-orthogonal designs will be extensions. Here $N_{t-1} = N_2 = \binom{k}{2}\frac{v-k}{k-2}$. (An extension of a Steiner system of type t-d-n is one of type $(t + e) - (d + e) - (n + e)$ such that the contraction of the latter on e points is the original system.)

Set

$$N_1 = \left\{ D \epsilon \mathcal{D};\ |D \cap D_0| = 1 \right\}$$

where $D_0 \epsilon \mathcal{D}$. Again, an easy counting argument shows that

$$N_1 = k \left| \frac{(v-1)\ (v-2)}{(k-1)\ (k-2)} - 1 \right| - 2N_2$$

Now, N_1 must be 0. Hence we conclude that

$$\frac{(k)\ (k-1)\ (v-k)}{(k-2)} = k \left| \frac{(v-1)\ (v-2)}{(k-1)\ (k-2)} - 1 \right|$$

or that

$$(k-1)^2 (v-k) = v^2 - k^2 - 3v + 3k$$

or

$$v = k^2 - 3k + 4$$

Thus, v is determined by k. (In the more general case a similar argument shows that v is determined by k and t.)

The fact that we have a Steiner system implies that k-2 divides v-2, that (k-1) (k-2) divides (v-1) (v-2) and that k(k-1)(k-2) divides v(v-1)(v-2). But v-2 = (k-1) (k-2) and hence we conclude that k divides v(v-1); thus k divides 12. Thus, since k is even, k is 2, 4, 6, or 12. For k = 2, v is 2, a trivial case. The cases k = 4 and k = 6 are well understood; the case k = 12 is the only undecided case. Because of known extension properties which come from easy counting arguments we are able to sum up the preceding discussion in:

THEOREM 1. Let $(S, \mathcal{D})$ be a self-orthogonal Steiner system with parameters t, k, and v. Suppose $t > 1$ and $k < v$. Then one of the following four cases occurs:

a. t = 3, k = 4, v = 8 and the design is the unique extension of the projective plane of order two or, in coding terms, the quadruple system associated with the (8, 4) extended Hamming code.

b. t = 3, k = 6, v = 22 and the design is the unique extension of the projective plane of order four or, in other words, the design associated with the Mathieu group M_{22}.

c. $t = 5$, $k = 8$; $v = 24$ and the design is the unique Steiner system with those parameters, the one associated with M_{24}. Note that this design is that of b. twice extended; and it is the only self-orthogonal Steiner system with $t > 3$ since the only other case is

d. $t = 3$, $k = 12$, $v = 112$.

It is, or course, unknown at this time whether a Steiner system with the parameters of a. exists. If it does, it is necessarily an extension of a projective plane of order ten and has no further extensions. It was this numerical anomaly that titillated our interest in the possibility of a projective plane of order ten being constructible within the framework of algebraic coding theory. Our discussion to follow was motivated by cases a. and b. above. The preceding discussion also affords a proof of the following.

COROLLARY. The only extendable projective planes are those of order two, four, and possibly ten.

Proof. Such an extension is easily seen to be a self-orthogonal design with $t = 3$. (One simply computes N_1 and sees it is 0.)

2. The Linear Span of a Projective Plane.

Let $(S,\mathcal{D})$ be a finite projective plane of order n. Thus, $(S,\mathcal{D})$ is a 2-design with $\lambda = 1$, $|S| = n^2 + n + 1$ and $|D| = n + 1$ for $D \in \mathcal{D}$. In $GF(2)^S$ we consider the collection of characteristic functions for each $D \in \mathcal{D}$ and set A equal to their linear span. Thus, A is the row-space over GF(2) of the incidence matrix of the plane. Since the rational determinant of the incidence matrix of a plane of order n is

$$n^{(n^2 + n)/2}\,(n + 1)$$

the matrix is always singular over GF(2). In case n is odd, A consists precisely of a kernel of the linear functional which sums the coordinates of $GF(2)^S$; i.e., the space of even-weight vectors. (This is trivial to see directly since the mod 2 sum of the $n + 1$ lines through a point is the vector with 0 at that point and 1's elsewhere; these clearly generate the even-weight subcode.) Here we are interested in the case of n even. The dimension of A clearly depends on the congruence of n mod 4. We have the

PROPOSITION 1. If $n \equiv 2(4)$, then $\dim A = \dfrac{n^2 + n + 2}{2}$

In fact, we give an elementary proof of the fact that if $\dim A = r$, then $2^{n^2 + n + 1 - r}$ divides $n^{(n^2 + n)/2}$; where we only assume n is even. Then $n \equiv 2(4)$ will imply $r \geq (n^2 + n + 2)/2$.

Proof. Let M be the incidence matrix of the plane. View M as a linear transformation over GF(2) of $GF(2)^S$ into $GF(2)^S$. Now dim Ker $M = n^2 + n + 1 - r = k$, say. Let $a_1, \ldots,$ a_k be row vectors in this kernel and set

$$N = \left(\begin{array}{c|c} \multicolumn{2}{c}{a_1} \\ \multicolumn{2}{c}{\vdots} \\ \multicolumn{2}{c}{a_k} \\ \hline O_k & I \end{array}\right)$$

where we rearrange coordinates so that

$$a_i = (0, 0, \ldots, \underset{\text{i-th coordinate}}{\overset{k}{1}}, *, \ldots *; *, *, \ldots . *).$$

Now view M and N rationally. Clearly det N = 1, since it is upper triangular with 1's on the diagonal and NM has its first k rows all multiples of 2. Thus, 2^k divides det NM = det $M = n^{(n^2 + n)/2} (n + 1)$ and hence the Proposition, since 2 divides n once exactly.

A more elegant proof uses the result from the theory of elementary divisors that any $m \times m$ integer matrix can, by pre- and post-multiplication by unimodular matrices, be put in the form Diag $(d_1, d_2, \ldots, d_m)$ where $d_1 | d_2 | \ldots | d_m$. Clearly, then, for an incidence matrix of a projective plane the mod p rank of the matrix is at least $n^2 + n + 1 - s$, where p^s but no higher power of p divides $n^{(n^2 + n)/2} (n + 1)$, since at most s of the d_i's can be divisible by p.

Since, for n even, dim $A \leq \frac{n^2 + n + 2}{2}$ (this because with an overall parity check added A is self-orthogonal), clearly, we immediately have the Proposition, and moreover our last remark yields

PROPOSITION 2. Let $(S, \mathscr{D})$ be a projective plane of order $n \equiv 2 \pmod 4$. Let A* be the subspace of $GF(2)^{S \cup \{*\}}$, generated by all vectors which are characteristic functions of $D \cup \{*\}$, $D \in \mathscr{D}$. Then A* is a half-dimensional self-orthogonal subspace of $GF(2)^{n^2 + n + 2}$.

Remarks: 1. A* is simply A with an overall parity check added.

2. In case A comes from a plane of order $\equiv 0 \pmod 4$, the dimension can go down. For example, for n = 4, the dimension of A is 10, not 11 (see subsection 3 following). For a related discussion of the possible dimensions of the linear span of difference sets, see [1, 2].

Although we are interested in the case $n = 10$, we proceed more generally under the assumption that $n \equiv 2 \pmod 4$. Let A be as above. From Proposition 2 follows immediately the

COROLLARY 1. Every vector in A has weight congruent to 0 or 3 modulo 4, and an even-weight vector is in A if and only if it intersects each line evenly, an odd-weight vector is in A if and only if it intersects each line oddly.

We next determine the minimum weight in A.

PROPOSITION 3. The minimum weight in A is $n + 1$. Moreover, every vector of weight $n + 1$ in A is a line of the plane.

Proof. Suppose v in A has weight less than $n + 1$. If $d =$ weight v is odd, all $n^2 + n + 1$ lines meet v (i.e., v and a line have a 1 in common). But at most $d(n+1)$ lines meet v, a contradiction. If d is even, each line through a fixed point of v must meet v again. Hence, the weight of v is greater than $n + 1$. If v in A has weight $n + 1$, there is some line D of the plane meeting v at least twice. But then the n other lines through a point on D but not on v (if such a point exists) must each meet v at least once, an impossibility. Hence $v = D$.

DEFINITION. An S-arc of a projective plane is a set of S points no three of which are collinear.

An easy argument shows that S-arcs can exist only if $S \leq n + 2$. An $(n + 2)$ arc is here called an oval.

PROPOSITION 4. The vectors of weight $n + 2$ in A are precisely the ovals of the projective plane.

Proof. The arguments are as above and very easy.

COROLLARY 2. In a projective plane of order $n \equiv 2 \pmod 4$, any two $n + 2$ arcs meet evenly, in at most $\frac{n+2}{2}$ points.

(This corollary is immediate from Propositions 3 and 4.)

The above results furnish a new proof of the following.

PROPOSITION 5. There do not exist projective planes of order congruent to 6 modulo 8; in particular, there does not exist a projective plane of order 6.

Proof. Consider A* for such a plane. It is self-orthogonal, half-dimensional, and all vectors have weight congruent to 0 modulo 4. It is known either from the theory of quadratic forms or can be deduced immediately from Gleason's solution of the MacWilliams equations that in such a situation the ambient space has dimension congruent to 0 modulo 8. But this dimension is $n^2 + n + 2 \equiv 4 \bmod 8$, a contradiction.

We now restrict ourselves to $n = 10$. Thus, A is a 56-dimensional subspace of $GF(2)^{111}$; i.e., a (111, 56) code over GF(2) and A* is a 56-dimensional self-orthogonal subspace of $GF(2)^{112}$ and simply A with an overall parity check added. The weight 11 vectors of A are simply the lines of the plane of order 10, the vectors of weight 12 in A the ovals of the plane of order 10. A has precisely 111 weight 11 vectors.

A computation performed by MacWilliams, Sloane, and Thompson [3] has shown that A has no vectors of weight 15. This fact, under the additional strong assumption that the weight 12 vectors of A* form the design of case d. in Theorem 1 – namely, a Steiner system of type $t = 3$, $v = n^2 + n + 2$, $k = 12$ (this assumption is equivalent to assuming that there is a projective plane of order 10 with an extension) – yields a unique weight distribution for A*. It is

Weight	Number of Vectors
0 and 112	1
12 and 100	1036
16 and 96	0
20 and 92	868,560
24 and 88	111,965,910
28 and 84	10,847,119,360
32 and 80	581,085,136,170
36 and 76	15,631,795,001,900
40 and 72	219,372,154,900,360
44 and 68	1,662,571,548,245,160
48 and 64	6,958,514,212,873,685
52 and 60	16,330,986,833,984,592
56	21,682,256,857,734,468

At the present time an attempt to construct such an A* is underway. The methods being employed do not prejudice the question of existence. An instance of these methods is recorded in subsection 4.

3. The Linear Span over GF(2) of the Lines of the 21-Point Plane.

The lines of this plane can be obtained from the Steiner System of type 5-8-24 by contraction, hence from the extended Golay (24, 12) code over GF(2). It is easy to show with counting arguments (using the 5-design properties of the weight 8 and 12 vectors) that the contracted code, a (21, 12) code over GF(2), has the following weight distribution:

Weight	Number of vectors
0	1
5	21
6	168
7	360
8	210
9	280
10	1008
11	1008
12	280
13	210
14	360
15	168
16	21
21	1

Clearly, the 21 weight 5 vectors (the lines of the 21-point projective plane) are orthogonal to the subcode of even-weight vectors. This code is a (21, 11) of course; its 168 weight 6 vectors are precisely the ovals of the 21-point plane.

Computing directly from an incidence matrix of the 21-point plane, one sees that the linear span is 10-dimensional. Hence, the span of the lines of the plane is precisely the code orthogonal to the even-weight subcode (which has dimension 11).

Since the weight 8 and weight 12 vectors of the (21, 12) come from weight 8 and 12 vectors, respectively, of the (24, 12) with zeroes at the contracted components, they are clearly orthogonal to all vectors in sight. Hence, the linear span of the 21-point plane has exactly 210 weight 8 (and hence weight 13) vectors and exactly 280 weight 12 (and hence weight 9) vectors. This exhausts the code. Hence, the weight distribution of the linear span of the lines of the 21-point projective plane is:

Weight	Number of Vectors
0	1
5	21
8	210
9	280
12	280
13	210
16	21
21	1

Observe that a weight 8 vector arises precisely as the sum of two lines since there are 210 such configurations.

4. The Row Space of the Z-Matrix.

Let Z be the matrix whose columns are 112 ovals of the 21-point plane, precisely those ovals with a 1 at ∞ and another at either 0 or 1, thinking of the plane as coming from a contraction of the (24, 12) extended Golay code, the coordinates contracted on being ∞, 0, 1. (The other 56 ovals of the plane have a 0 at ∞ and 1's at 0 and 1.)

Because these 112 ovals form a 2-design ($2 \cdot M_{21}$ acts transitively on them), each of the 21 rows of Z has weight 32 and the sum of any two distinct rows has weight 48 (since $\lambda = 8$ for the 2-design).

Since the columns of this matrix span the even-weight subcode of the (21, 12), the rank of the matrix is 11, a fact easily seen upon exhibiting the matrix using Todd's table [4].

We now determine the weight distribution of Z's row space, a (112, 11) code over GF(2).

Since the columns generate the space orthogonal to the span of the lines of the 21-point projective plane, any relation among the rows of Z corresponds to a vector in the span of the 21-point plane. Since there are no weight 2 or 4 vectors in the span of the 21-point plane, each pair of distinct rows yields a different weight 48 vector.

Now, any vector in the row span of Z is the sum of rows corresponding to a subset of the plane no three of whose points are collinear, since any three collinear points could be replaced by the other two points of the line containing them.

Any four points in this plane, no three of which are collinear, are in a unique oval. In general, in any plane of even order n, any n + 1 points in general position lie in a unique oval. And, in general, by looking at all the lines through a point, we see that there can be at most n + 2 points in general position.

One computes directly from the fact that each triple of non-collinear points is contained in precisely 3 ovals, one each from the three classes represented by

$$\begin{array}{c|ccc} \infty & 1 & 1 & 0 \\ 0 & 1 & 0 & 1 \\ 1 & 0 & 1 & 1 \end{array}$$

that the sum of these rows is a weight 56 vector, since the third of the three rows meets the intersection of the first two precisely twice and each row precisely eight times.

Clearly, an oval of type $\begin{matrix}0\\1\\1\end{matrix}$ meets each column of Z oddly and hence such an oval yields the all-1 vector. Any five points of such an oval, therefore, yield the complement of a row while any four points of such an oval yield the complement of a sum of two rows; any three yield, of course, a weight 56 vector.

By inspection (since they are all equivalent under $2 \cdot M_{21}$, one inspection suffices), any four points or any five points of chosen ovals (i.e., of type $\begin{matrix}1\\0\\1\end{matrix}$ and $\begin{matrix}1\\1\\0\end{matrix}$) yield weight 56 vectors. Clearly, an oval of type $\begin{matrix}1\\0\\1\end{matrix}$ or $\begin{matrix}1\\1\\0\end{matrix}$ yields a weight 56 vector since it meets its own type evenly and the other type oddly. Thus, the only weights that appear are 0, 32, 48, 56, 64, 80, 112 and we know there are 21 weight 32's exactly (and hence 21 weight 80's exactly and $\binom{21}{2}$= 210 weight 48's exactly (and hence 210 weight 64's exactly). By elimination there are 1584 weight 56 vectors. Tabularly, the row space of Z has the following weight distribution.

Weight	Number of Vectors
0	1
32	21
48	210
56	1584
64	210
80	21
112	1

References

[1] J. M. Goethals and P. Delsarte, "On a Class of Majority-Logic Decodable Cyclic Codes," IEEE Trans. Information Theory IT-14 (1968), pp. 182-188.

[2] R. L. Graham and F. J. MacWilliams, "On the Number of Information Symbols in Difference-Set Cyclic Codes," Bell Sys. Tech. J., 45 (1966), pp. 1057-1070.

[3] F. J. MacWilliams, N.J.A. Sloane, and J. G. Thompson, "On the Existence of a Projective Plane of Order 10," Internal Memo, Bell Telephone Laboratories, Murray Hill, N.J., September 1970.

[4] J. A. Todd, "A Representation of the Mathieu group M_{24} as a Collineation Group," Annali di Matematica pura ed applicata, (IV), Vol. LXXI (1966), pp. 199-238.

PART III

T-DESIGN DECODING AND THE (48, 24) BINARY QR CODE

1. Introduction.

In our 1969 Report [3, III, 3] we presented a majority-logic method for decoding the Golay (24, 12) binary code, a 5-design code, involving use of the 2-design formed by the minimum-weight code-vectors with 1's at a given pair of coordinate places. This method allowed correction of all errors of weight 3 or less and detection of all errors of weight 4, which together exhaust the coset leaders of the code. Here we present a method for decoding binary t-design codes by means of the 1-design formed by the minimum-weight vectors. This was done for the (24, 12) code by Goethals [5] and has since been generalized by him [6] independent of our work, although we expect eventually to publish this work jointly with him.

The general tactic is simple to describe. If the orthogonal to a code A has a t-design among its vectors of a given weight, say with parameters λ; t-w-n (see [2] for definitions and examples), then this design may be regarded also as a t-1 or t-2, ..., or 1-design with parameters

$$\begin{array}{l} \lambda = \lambda_t;\ t\text{-}w\text{-}n \\ \lambda_{t-1};\ (t-1)\text{-}w\text{-}n \\ \quad \cdot\ \cdot\ \cdot \\ \lambda_1;\ 1\text{-}w\text{-}n \end{array} \qquad (1)$$

given by the simple relations

$$\lambda_i = \lambda_t \frac{(n-i)_{t-i}}{(d-i)_{t-i}}\ , \quad i = 0, 1, \ldots, t \qquad (2)$$

$(N)_i$ stands for the familiar descending product $N(N-1)\ldots(N - i + i)$. The general tactic in this decoding method is to compute the dot-products of the λ_1 vectors of the 1-design which have 1's at a given coordinate place p with a received vector v + E, where v (from A) was sent, and the error E was "committed" by the channel. The outcome is the dot products with E, a vector really of λ_1 0's and 1's; we are interested only in its weight. We compute theoretically this weight for all possible cases for e (= weight of E) running from 1 up to some value, say, e_0. If these weights are different from each other, then all cases are distinguishable from each other via this procedure: and so the code A will correct all errors of weight e_0 or less; in particular, A has minimum distance at least $2e_0 + 1$.

2. Calculation of the Decoding Table, and Some Consequences.

The job here is simply to identify the cases and compute the weight of the λ_1-length vector mentioned above for each case. That is, we seek the number of vectors among the chosen λ_1 in the design from the orthogonal code to A which have dot-product 1 with the assumed error-vector, and we shall call this number the outcome.

Let p stand for the coordinate position being checked; that is, the λ_1 vectors used in the dot-product calculation all have a 1 at p. Let S stand for the set of these λ_1 vectors of B. Then, if the error has weight 1, the outcome is λ_1 if the error is at p, but is λ_2 if the error is not at p. If the error has weight 2, then the outcome is $\lambda_1 - \lambda_2$ if the error has a 1 at p, and it is $2(\lambda_2 - \lambda_3)$ if position p is not in error. These results are calculated by simple inclusion-exclusion arguments. For example, assuming $t \geq 3$, the number $2(\lambda_2 - \lambda_3)$ arises as follows: let the error be at p', p'', neither equal to p. There are λ_2 coverings of p and p', and λ_2 of p and p''; but coverings of all three, λ_3 in number, have been counted twice but have dot-product 0. Thus $2\lambda_2 - 2\lambda_3$.

LEMMA 1. Let $t \geq e$. The outcome for an error of weight e covering p is λ_1 less the outcome for an error of weight e - 1 not covering p.

Proof. It is almost self-evident; the λ_1 vectors covering p have dot-product 1 with an error vector E of weight e covering p if and only if they have dot-product 0 with the vector of weight e - 1 defined by removing p from E (we identify a vector with the set of coordinate places where it is 1 when convenient); the latter are all those not having dot-product 1 on $E - \{p\}$, hence the conclusion.

We present the results for $t \leq 5$ in Table III-1, in which the entries are the outcomes as defined above.

TABLE III-1. DECODING TABLE:OUTCOME OF DOT PRODUCTS ON ERROR VECTORS

Valid for	Weight Error Vector	Position p is in Error	Not in Error
	1	λ_1	λ_2
$t \geq 2$	2	$\lambda_1 - \lambda_2$	$2(\lambda_2 - \lambda_3)$
$t \geq 3$	3	$\lambda_1 - 2\lambda_2 + 2\lambda_3$	$3\lambda_2 - 6\lambda_3 + 4\lambda_4$
$t \geq 4$	4	$\lambda_1 - 3\lambda_2 + 6\lambda_3 - 4\lambda_4$	$4(\lambda_2 - 3\lambda_3 + 4\lambda_4 - 2\lambda_5)$
$t \geq 5$	5	$\lambda_1 - 4(\lambda_2 - 3\lambda_3 + 4\lambda_4 - 2\lambda_5)$	$16\mu + 5(\lambda_2 - 4\lambda_3 + 8\lambda_4 - 8\lambda_5)$
	6	$\lambda_1 - 16\mu - 5(\lambda_2 - 4\lambda_3 + 8\lambda_4 - 8\lambda_5)$	$16\nu + 2(3\lambda_2 - 15\lambda_3 + 40\lambda_4 - 60\lambda_5)$

The left-hand column of entries is calculated from Lemma 1 and from the right-hand entries, which are derived by the kind of inclusion-exclusion argument given above. The entries in the line for e = 6 will be explained in a moment. We now discuss the right-hand entry for e = 5.

We assume t = 5. μ is defined for each 6-subset of coordinates as the exact number of code-vectors of B (of the weight class forming the t-design in use) having 1's at all coordinates of 6-subset. In the right-hand entry for e = 5, the 6-subset is $\{p\} \cup E$, where E is the error vector of weight 5. The outcome is the number of members of S meeting E exactly 1 or 3 or 5 times. We indicate the derivation. $5\lambda_2$ is the number of members of S meeting E once or more. Since there are 10 2-subsets of E, and each is counted twice in the $5\lambda_2$ term, we exclude all the members of S meeting E twice or more by subtracting $20\lambda_3$. Every member of S meeting E exactly three times, however, was counted thrice in $5\lambda_2$ and 6 times in $20\lambda_3$. By adding $4\binom{5}{3}\lambda_4 = 40\lambda_4$, we include all members of S meeting E 3 or more times. Those members of S meeting E exactly 4 times were counted 4 times in $5\lambda_2$, 12 times in $20\lambda_3$ and 16 times $40\lambda_4$, hence we exclude the members of S meeting E 4 or more times by subtracting $8\binom{5}{4}\lambda_5 = 40\lambda_5$. Finally, there are by definition μ members of S meeting E 5 times; each of these was counted 5 times in $5\lambda_2$ $2\binom{5}{2} = 20$ times in $20\lambda_3$, $4\binom{5}{3} = 40$ times in $40\lambda_4$ and $8\binom{5}{4} = 40$ times in $40\lambda_5$. The net is -15, so we add 16μ.

The argument of Lemma 1 applies here even though we do not assume a 6-design, hence our entry in the left at e = 6.

In the entry on the right at e = 6, ν is defined as the number of members of S which meet the weight-6 error E on exactly 5 spots. By an argument entirely similar to the previous one, we calculate the outcome. Note that the number of members of S which meet E in all six spots is of no interest here, because they have dot-product 0.

We now state a Theorem based on this table and investigate some matters growing out of that Theorem before returning to our decoding problem.

THEOREM 1. Let A be a binary code whose orthogonal contains a t-design. If the entries in the first t-1 rows of Table III-1 for this code are all different from each other, then the minimum weight d in A is at least 2t-1. Moreover, although the t-th row of the table may have multiple entries, if these are all distinct from each other and from those above, then d = 2t + 1.

Proof. There exists a decoding algorithm for A correcting any t - 1 (or t) errors.

COROLLARY 1. The orthogonal of the non-trivial binary 3-design code has minimum weight 5 or more unless the code is the extended maximal length $(2^k, k)$ code.

Proof. In Table III-1 we investigate the possibility of equalities among the entries in the first two rows, making use of (2), of course.

1. If $\lambda_1 = \lambda_2$, then the design is trivial; i.e., it either consists of the empty set ($\lambda_1 = 0$) or has precisely one block consisting of the underlying set (d = n).

2. If $\lambda_1 - \lambda_2 = 2(\lambda_2 - \lambda_3)$ then, expressing everything in terms of λ_3, we have one of the following 3 cases:

   a. $\lambda_3 = 0$ and the design is the empty set;
   b. n = d, and the design consists of one block;
   c. n = 2d.

This case can occur; e.g., A is the orthogonal to the extended Hamming code B. B has minimum weight 4, so all double errors are ambiguous.

These results follow since the equation

$$\frac{n-1}{d-1} + \frac{2(d-2)}{(n-2)} = 3$$

as a quadratic in n has the solutions n = d and n = 2d.

3. $\lambda_1 - \lambda_2 = \lambda_2$ implies $n = 2d - 1$, a contradiction, because the code must be the maximal length code, as we now prove.

PROPOSITION 1. The binary (n, k) code with $n = 2d - 1$ in which the weight d vectors form a 2-design is the maximal length code.

Proof. There can be no repeated columns in the code (i.e., no two coordinates are identical) because this would imply $\lambda_1 = \lambda_2$, hence from (2) that $n = d$, hence $d = 1 = n$. No coordinate functions are 0 or there would be no design. From Plotkin's bound

$$d \leq n2^{k-1}/(2^k - 1)$$

it follows that $n \geq 2^k - 1$; hence $n = 2^k - 1$ since no coordinate functions may be duplicated - Q.E.D.

This result complements our Corollary 3 in [1].

Such a code is not a 3-design because its orthogonal, the Hamming code, is not a 3-design [7].

We now complete the proof of our Corollary.

4. $\lambda_1 = 2(\lambda_2 - \lambda_3)$ implies

$$\frac{n-1}{d-1} - 2 = -2\frac{d-2}{n-2}$$

or if $d > 2$, the left side is negative and thus

$$\frac{n+1}{2} < d,$$

which contradicts the bound $d \leq \frac{n+1}{2}$ [3(6)]. If $d = 2$, then $n = 3$, a trivial case.

This completes the proof of the Corollary, and we return to our decoding topic.

3. Application to the (48, 24) QR Code.

We now specialize the problem to the (48, 24) extended binary quadratic residue code.

This code is self-orthogonal, of minimum weight 12, and all weight-classes form 5-designs [2]. We shall work with the weight 12 vectors, which are a 5-design with parameters 8; 5-12-48. It follows from (2) that

$\lambda_5 = 8$

$\lambda_4 = 44$

$\lambda_3 = 220$

$\lambda_2 = 1012$

$\lambda_1 = 4324$

We now :ill Table III-1 with these values for the λ' s.

TABLE III-2. THE DECODING TABLE FOR THE (48, 24) CODE

	Position p is		
Weight of Error	In Error	Not in Error	
1	4324	1012	
2	3312	1584	
3	2740	1892	
4	2432	2048	
5	2276	$2100 + 16\mu$	$(0 \le \mu \le 5)$
6	$2224-16\mu$	$2032 + 16\nu$	

It is apparent that all the entries are indeed different, except perhaps that those involving μ or ν will produce a coincidence somewhere. We recall the definitions of μ and ν and then make some needed remarks. For a given 6-set μ is the number of weight 12 vectors of the (48, 24) code with 1' s at all the spots of the 6-set. The 6-sets understood in Table III-2 are $\{p\} \cup E$ and E on lines 5 and 6, respectively. ν is defined as follows: for a given 6-set E not containing p, ν is the number of 12-clubs (code-vectors of weight 12) with 1' s at p and at exactly 5 spots of E.

Thus, in particular, ν is at most 48 (= $6\lambda_5$).

REMARK 1. All we need from the table is the condition that no number appear in both the left- and right-hand columns. This suffices to determine whether there is an error at p.

REMARK 2.

a. If an error of weight 6 is contained in one or more 12-clubs, then it cannot be corrected by any method in the sense that it is not a unique leader in its coset. Therefore, for each positive μ, provided there is a 6-set contained in exactly μ 12-clubs, we should find the value $2224 - 16\mu$ on both sides of the table, and on line 6. Specifically, if E and E' are 6-sets whose union is a 12-club, and if p is in E, and $\mu = \mu(E)$, $\nu = \nu(E')$, the outcome for the error E must be the same as that for the error E'. Therefore

$$2224 - 16\mu = 2032 + 16\nu,$$

which is equivalent to $\mu + \nu = 12$.

b. Since no two 12-clubs can meet in more than six places, an upper bound for μ is 7. Thus, for a 6-set E with a positive μ, the value of ν for the 6-sets E' such that $E \cup E'$ is a 12-club is at least 5, but at most 11.

Ambiguous Cases.

i. We have just seen that an error of weight 6 is uncorrectable when it has positive μ and that this fact is reflected in the outcome of our decoding procedure.

ii. The entries $2100 + 16\mu$ on line 5 at the right can never coincide with any of those on the left, for by Remark 2 b. μ is at most 7, hence $2100 + 16\mu$ is at most 2212; and $2224 - 16\mu'$ cannot equal $2100 + 16\mu$ since $2100 \not\equiv 2224 \pmod{16}$.

iii. For positive μ we know that $\nu \leq 11$. Therefore, the right-hand entry $2032 + 16\nu$ is at most 2208 when $\mu > 0$, showing that none of these values can also appear on the left.

iv. But for $\mu = 0$, we do not yet have any bounds on ν except the obvious one already mentioned ($\nu \leq 48$), which gives 2800 as an upper bound for $2032 + 16\nu$. On the left, the entry 2740 is not 0 mod 16, and neither is 2276; 2432 is 0 mod 16, however, and so is 2032. Thus $\nu = 25$ would give ambiguity if it arose.

v. The only remaining possibility is an error of weight 6 with $\mu = 0$. It is a unique coset leader and ought to be correctable, but the left-hand entry on line 6, 2224, would coincide with the right-hand entry if the value of ν were 12.

The remainder of this account will deal with this only remaining unsettled case, namely, the value of ν for the error of weight 6 which is not contained in any 12-club, for we prove in subsection 4 that $\nu < 25$.

We state our findings.

PROPOSITION 2. For every 6-set E of coordinate places not contained in any 12-club and every p not in E, the value of ν is 8.

Proof. By computer. The program is described in the Appendix to this part.

COROLLARY 2. The ambiguities of cases iv. and v. do not in reality arise. The decoding procedure corrects all errors of weight 5 or less and all errors of weight 6 which are unique leaders of their coset.

COROLLARY 3. No error of weight greater than 6 is a unique leader of its coset.

Proof. Suppose the contrary, that a vector E' of weight $w \geq 7$ is the unique leader of its coset. There can be no 12-club containing E', and if E is any 6-subset of E', then there cannot be any 12-club containing E, for it would yield another leader of weight w on being added to E'. But if E is one such subset of E', the Proposition states that there are 12-clubs meeting E' in a 6-set.

Therefore the decoding procedure corrects all errors which are unique leaders in their cosets.

It remains to determine how many correctable errors there are; the only difficulty is to find how many of weight 6. The answer is set forth in Table III-3.

TABLE III-3. NUMBER OF CORRECTABLE ERRORS OF EACH WEIGHT

Weight w	
0	1
1	48
2	1,128
3	17,296
4	194,580
5	1,712,304
6	2,334,960*
$w \geq 7$	0
Total	4,415,947

About 18 percent (= 2,334,960 ÷ $\binom{48}{6}$) of errors of weight 6 are correctable.

There are approximately 10 million uncorrectable errors of weight 6 distributed in 4,112,124* cosets. All the rest of the cosets, in number about 8 million, have more than one leader of weight 7 or more. The total number of cosets is 2^{24} = 16,777,216.

The μ-distribution of 6-sets is given in Table III-4.

TABLE III-4. NUMBER OF 6-SETS CONTAINED IN EXACTLY μ 12-CLUBS*

μ	
0	2,334,960
1	5,629,848
2	2,750,064
3	1,400,976
4	129,720
5	25,944
$\mu \geq 6$	0
Total	$\binom{48}{6}$

*These values were obtained by computer (see Appendix).

4. Theoretical Results.

Although we were forced to resort to computer for some of our results, we have a partial theoretical result which we now present. It is not dependent on our computer findings.

LEMMA 2. Let E be an error of weight 6 not contained in any 12-club. Let p be a point not in E. Then ν (p, E) < 25.

Proof. ν is defined as the total number of 12-clubs which meet E in 5 places and which cover p. Let $N_1, \ldots, N_6$ be the (mutually disjoint) classes of 12-clubs which have the the form 011111, 101111, etc., on E and have a 1 at p. Let $n_1, \ldots, n_6$ be the cardinality of $N_1, \ldots, N_6$, respectively. Then, denoting E by $p_1, \ldots, p_6$, we see that

1. $n_i \le 6$ for each i. For if n_i were 7 for some i, there would be 7 12-clubs covering the 6 points p, $p_1, \ldots, \hat{p}_i, \ldots, p_6$, and having 0 at p_i. These would have to cover all the remainder of the 48 points including p_i, a contradiction.

2. $n_i \le 5$ for each i. For if n_i were 6 for some i, then the sum of all 6 weight 12's would be a vector of weight 36, the complement of which would cover all 7 points p, $p_1, \ldots, p_6$, a contradiction to our assumption that $p_1, \ldots, p_6$ is not contained in any weight 12 code vector.

3. $n_j = 5$ implies $n_i \le 3$ for all $i \ne j$. Alternately, $n_i + n_j \le 8$ for all $i \ne j$. For $N_i \cup N_j$ is a class of 12-clubs with 1's at the 5 points p, $p_1, \ldots, \hat{p}_i, \ldots, \hat{p}_j, \ldots, p_6$, and $\lambda_5 = 8$.

4. Thus $\nu = n_1 + \ldots + n_6 < 25$. For if $n_i = 5$ for some i, then all n_j, for $j \ne i$, are 3; thus $\nu = 20$. If $n_i \le 4$ for all i, then $\nu \le 24$.

Thus one of our possible ambiguities is eliminated.

5. The Decoding Procedure.

First, perform the 4,324 dot products consisting of all the weight-12 parity checks which cover the first coordinate of the code.

The outcome is the number of parity-check values equal to 1. If there are 6 or fewer errors present, act according to the following directions:

(1) If outcome is 0, no errors are present.

(2) If outcome is 2224 or greater, then the value in the first coordinate is in error. Change the value, cycle the vector once, perform the 4,324 dot products, and go to (1).

(3) If outcome is 2208, 2192, 2176, or 2148, then an uncorrectable error of weight 6 is present. Hence, declare the vector in error and thus detect but do not correct it.

(4) If the outcome is 2160, cycle and repeat the checks. If the outcome is always 2160, then there is an uncorrectable error of weight 6. Otherwise, the outcome will be 2224 at various places, in which case proceed as in (2).

(5) If the (positive) outcome is 2132 or less, or if it is 2148, 2164, or 2180, then the first position is correct but there is present a correctable error of weight 5 or less, which will be corrected on repetition of these cycling and parity-check operations.

This procedure corrects all errors of weight 5 or less and 18 percent of all errors of weight 6. (There are no other correctable errors.) It detects all other errors of weight 6.

Steps (1) through (5) are easily derived from Tables III-2, III-3, III-4, Remark 2 and Proposition 2.

6. Appendix.

How the computer was used. A basis for the code, generated in 1966 for our research on 5-designs, was typed into storage. The $\lambda_3 = 220$ 12-clubs containing three fixed spots 0, 1, 2 were then generated and stored. Since the invariance group of the code is 3-set transitive, it sufficed to compute what we wanted on this tableau. The 14,190 3-subsets of $\{3, 4, \ldots, 47\}$, 47 standing for ∞, were then processed in turn:

1. The first action taken was to orbit the 3-subset under the group of order 3 fixing the tableau, generated by $\begin{pmatrix} 23 & 1 \\ 11 & 1 \end{pmatrix}$, which permutes 0 to 1 to 2 to 0. If any member of the orbit of the triple had been processed already, the present triple was dropped and the next one taken up.

2. The next process was to compute μ for the triple α, β, γ, which passed test 1. The three columns of the tableau, having been converted to words, were simply "anded" together, and the weight of the resulting word was μ for the 6-set $\{0, 1, 2, \alpha, \beta, \gamma\}$. The μ counter was bumped, and whether $\{\alpha, \beta, \gamma\}$ was fixed by the 3-group above was counted also.

3. If $\mu = 0$, the value of ν was found. This required "anding" α, β, and γ in pairs and for the "and" of each pair, computing the "and" with each of the 42 other columns J, and then the weight of the result, recorded as a function of J. After that, a permutation in PSL_2 (47) carrying $\{0, 1, 2\}$ to $\{\alpha, \beta, \gamma\}$ was calculated (see below) and performed on the columns of the tableau. Then, after columns $\{0, 1, 2\}$ and $\{\alpha, \beta, \gamma\}$ were interchanged, the same routine was run again. An instruction to print and pause if ν were not 8 for any J was present, but was never executed.

The transformation $\begin{pmatrix} a & b \\ c & d \end{pmatrix}$, where

$$\begin{aligned} a &= S_2S_3 + S_1S_2 - 2S_1S_3 && (24S_2 - S_1) \\ b &= 2S_1(S_3 - S_2) && (S_1) \\ c &= 2S_2 - S_1 - S_3 && (23) \\ d &= 2(S_3 - S_2), && (1) \end{aligned}$$

is in PGL_2 (47) and carries $\{0, 1, 2\}$ to $\{S_1, S_2, S_3\}$, provided none of the S's is ∞. (Because our 3-sets were generated in the order 3, 4, 5; 3, 4, 6; ...; 3, 4, 47; 3, 5, 6; ...; 45, 46, 47, only S_3 could be $\infty = 47$, and the values for a, b, c, d in that case are in parentheses above.) The determinant ad-bc was tested for quadratic residuacity; when it was not a quadratic residue, the matrix was multiplied on the right by $\begin{pmatrix} -1 & 1 \\ 11 & 1 \end{pmatrix}$, which is in PGL_2 (47), not in PSL_2 (47) and has the effect (01)(2) on 0, 1, and 2.

A large number of hand checks of every part of the program was performed; also internal program checks were written in; the accuracy is highly recommended. Once the tableau was cast into proper form for processing, the whole program, written in Fortran, ran in four minutes of execution time (1900 kilocore-seconds used) on a PDP-10 time-sharing system.

A fast weight-counting routine, in which the effort is proportional to the weight, was used. Taken from [4, p. 16], the essential idea is that the least significant bit equalling 1 in the word W is made 0 while all other bits are unchanged by the step

W = W. AND. (W - 1).

In our problem the highest weight computed was 5.

The fact that ν has the constant value 8 whenever $\mu = 0$ was a surprise to us; it was suggested by some preliminary results typed out for hand checks, and then the instruction to print whether ν was different from 8 was written in.

The output of the program was the μ-distribution of the 3-subsets of $\{3, \ldots, 47\}$ according to whether or not they were fixed by the 3-group acting on the tableau. It is shown in Table III-5.

TABLE III-5. NUMBER OF TRIPLES*

$\mu=$	0	1	2	3	4	5	6	7
Not Fixed	899	2170	1060	536	50	10	0	0
Fixed	3	0	0	12	0	0	0	0

*The tables in the text were derived from this one by simple calculations.

References

[1] E. F. Assmus, Jr. and H. F. Mattson, Jr., "Error-Correcting Codes: an Axiomatic Approach," Information and Control 6 (1963) pp. 315-330; MR 31 (March 1966) No. 3251.

[2] E. F. Assmus, Jr. and H. F. Mattson, Jr., "New 5-Designs," J. Combinatorial Theory, 6 (1969), pp. 122-151.

[3] E. F. Assmus, Jr. and H. F. Mattson, Jr., Algebraic Theory of Codes II Scientific Report No. 1, 15 October 1969, Contract No. F19628-69-C-0068, Air Force Cambridge Research Laboratories, Bedford, Mass., AFCRL-69-0461.

[4] E. F. Beckenbach, (Ed.), Applied Combinatorial Mathematics, University of California Engineering and Physical Sciences Extension Series, John Wiley and and Sons, Inc., New York-London-Sydney, (1964).

[5] J. M. Goethals, On the Golay Perfect Binary Code, Report R93, October 1968, M. B. L. E. Laboratoire de Recherches, Brussels.

[6] J. M. Goethals, On t-Designs and Threshold Decoding, Institute of Statistics Mimeo Series, No. 600.29, Univ. of North Carolina, Chapel Hill, June 1970.

[7] Edward P. Shaughnessy, Associated t-Designs and Automorphism Groups of Certain Linear Codes, Ph.D. Thesis, Lehigh University, Bethlehem, Penn., 1969.

PART IV

ON THE (60, 30) QUADRATIC RESIDUE CODE OVER GF(3)

1. Introduction.

The code A of the title has been defined as one of an infinite class of extended quadratic residue codes, in [1] for example. That every code-vector in A has weight divisib'e by 3 is also proved there - the result follows from the fact that the code is self-orthogonal. The square-root bound on the minimum distance d comes from (see [1]) $d_1 (d_1 - 1) \geq 59 - 1$, where $d = 1 + d_1$; thus $d_1 > 8$, so $d > 9$; hence $d \geq 12$.

Pless has defined a class of self-orthogonal codes over GF(3) which includes a (60, 30) code for which the entire weight-distribution is known. The minimum distance in Pless's code is 18, and the distribution of weights is given by the entries in Table IV-1 [4]. This weight distribution is unique in that the MacWilliams equations have a unique solution for such (60, 30) codes when the minimum distance is 18 (see [5]).

Using a "contraction" mapping (in subsection 2 of this Part), we are able to show in subsection 3 that the code of the title has minimum weight either 12 or 18; that is, minimum weight 15 is not possible. Then, in subsection 4, we derive a simple result on the minimum weight in certain cyclic codes. This allows us to use a computer to determine that the minimum weight is 18 on examination of two million code-vectors. Thus, the code yields new 5-designs of block size 18, 21, ... , 33 on 60 points, and it has the same weight distribution as the Pless code in the following table.

TABLE IV-1. (60, 30) PLESS CODE*

Number of Code-Vectors	Weight
1	0
0	3
0	6
0	9
0	12
0	15
39 01080	18
2414 56320	21
88242 42960	24
17 20740 38080	27
185 03590 81824	30
1101 47500 94040	33
3609 93693 80880	36
6395 84677 67040	39
5927 89001 50800	42
2727 06401 78880	45
573 92571 92760	48
48 50290 78560	51
1 31440 38880	54
714 51360	57
41184	60

*From Reference [4].

Gleason [2] has found the generators of the weight distributions of all self-orthogonal codes over GF(3) (i.e., codes for which the orthogonal code has the same weight distribution). In polynomial form they are

$$P = y^4 + 8\,x^3 y$$

$$Q = (y^3 - x^3)^3 x^3 \qquad (1)$$

Here, x is the weight counter and y is the 0 counter. P gives the weight distribution of the (4, 2) code spanned by 1 1 1 0 and 1-1 0 1.

The weight distribution of the Golay (12, 6) code, for example, is written as $P^3 - 24Q$. The set of all products of P and Q of degree 60 yields all the solutions to the MacWilliams equations in that case, namely

$$P^{15},\ P^{12}Q,\ P^9Q^2,\ P^6Q^3,\ P^3Q^4,\ Q^5.$$

That is, any solution has the form

$$P^{15} + \sum_{1}^{5} \alpha_j P^{15-3i}\, Q^i$$

for appropriate constants $\alpha_1, \ldots, \alpha_5$. In order to produce $d \geq 12$ we need only consider the solutions

$$mP^3Q^4 + nQ^5 + P^{15} \qquad (2)$$

for integers m and n.

The tails of the weight distribution (2) for our code A are therefore:

Weight	Number of Code-Vectors	
12	m	
15	12m + n	
.	.	
.	.	
.	.	
60	-n + 41,184	(3)

for some proper choice of m and n. We will now explain a method which allows us to prove that m = 0 implies n = 0; i.e., that if $d > 12$, then $d = 18$.

2. The Contraction Mapping for Codes.

Suppose we have a concrete n-dimensional vector space $V = F^n$ over the field F. If we choose a set of m vectors from V and use these as linear functionals on V via the usual inner product we get, of course, a mapping ψ from V to F^m. If A is a code contained in V and if we restrict ψ to A, then we have mapping from A into F^m.

We now specialize the above situation: let A be an (n, k) code over GF(3) and let σ be an invariance of A. Set $V = GF(3)^n$ viewed as the containing space; set $r = \text{order } \sigma$. For our linear functionals we shall take certain vectors v with the property that either $\sigma v = v$ or $\sigma v = -v$. Sometimes there are no such non-zero v, however, so we must choose σ properly. In particular, we have the following two results.

LEMMA 1. If $4 | r$ and $\sigma^{r/2} = -1$, then there does not exist any non-zero vector v of V with either $\sigma v = v$ or $\sigma v = -v$.

Proof. $\sigma v = v$ implies $\sigma^{r/2} v = v$ implies $-v = v$ implies $v = 0$. And $\sigma v = -v$ implies $\sigma^{r/2} v = (-1)^{r/2} v$ implies $-v = v$ implies $v = 0$.

LEMMA 2. If $2 | r$ and $r/2$ is odd with $\sigma^{r/2} = -1$, then there does not exist any non-zero vector v of V with $\sigma v = v$. Moreover, if each cycle of $\bar{\sigma}$ is the same size, then for each cycle of $\bar{\sigma}$ ($\bar{\sigma}$ denotes the permutation part of σ) there is a unique non-zero (up to multiplication by ±1) vector v of V whose support is the given cycle with $\sigma v = -v$.

Proof. If $\sigma v = v$, then $\sigma^{r/2} v = v$ and $-v = v$ and $v = 0$. Clearly, $\sigma v = -v$ is possible. Let w be a vector with a 1 at one place in the given cycle and 0's elsewhere. Consider $w - \sigma w + \sigma^2 w - \ldots + \sigma^{r/2-1} w = v$. Clearly, the support of v is the given cycle. That $\sigma v = -v$ is clear. Suppose v' is another such with support v' contained in the given cycle. Then clearly the support is the whole cycle and, by adjusting if necessary, we can assure that $v - v'$ has a 0 on the cycle. But $\sigma(v - v') = v' - v = -(v - v')$. Therefore $v - v' = 0$.

REMARK. The Lemma is true even if the cycle sizes are different: one has to replace r/2 by s/2, where s is the order of σ restricted to the given cycle.

We now assume A is self-orthogonal and every cycle of $\bar{\sigma}$ is the same size, namely r/2. Thus $(r/2) | n$; say $(r/2)\, s = n$. The n coordinates split up into s cycles of size r/2. Let $v_1, \ldots, v_s$ be the unique (up to multiplication by ±1) vectors of V described by Lemma 2. We map $V = GF(3)^n$ to $W = GF(3)^s$ by

ψ: $v \mapsto (v \cdot v_1, v \cdot v_2, \ldots, v \cdot v_s)$, where $x \cdot y$ denotes the ordinary dot product.

THEOREM. $\psi(A)$ is a self-orthogonal subspace of W.

Proof. We view the coordinates as indexed by (i, j) where $1 \leq i \leq s$, $1 \leq j \leq r/2$, the orbits of $\bar{\sigma}$ being $\{(i, 1), (i, 2), \ldots, (i, r/2)\}$ for $i = 1, 2, \ldots, s$. Now, v_i is 0 at (i', j) for $i' \neq i$. So we view v_i as $(v_{i,1}, v_{i,2}, \ldots, v_{i,r/2})$. Suppose $x, y \in A$. Then

$$\psi(x) = \Big(\sum_{j=1}^{r/2} v_{1,j}x_{1,j}, \ldots, \sum_{j=1}^{r/2} v_{s,j}x_{s,j}\Big);$$

similarly for $\psi(y)$. Therefore

$$\psi(x) \cdot \psi(y) = \sum_{i=1}^{s} \sum_{j=1}^{r/2} \sum_{k=1}^{r/2} v_{i,j}v_{i,k}x_{i,j}y_{i,k} \qquad (*)$$

But $v_{i,j}^2 = 1$ for all i, j, and therefore

$\sum_{i=1}^{s} \sum_{j=1}^{r/2} v_{i,j}v_{i,j}x_{i,j}y_{i,j} = x \cdot y = 0$. We therefore view (*) as r/2 sums

$$\sum_{i=1}^{s} \sum_{j=1}^{r/2} v_{ij}v_{ij}x_{ij}y_{ij} + \sum_{i=1}^{s} \sum_{j=1}^{r/2} v_{ij}v_{i,j+1}x_{ij}y_{i,j+1} + \cdots +$$

$$+ \sum_{i=1}^{s} \sum_{j=1}^{r/2} v_{ij}v_{i,j+r/2-1}x_{ij}y_{i,j+r/2-1}$$

the second index taken mod r/2. Now suppose σ is such that σ sends (i, j) to $(i, j + 1)$ multiplied by ϵ_j, i.e., $(y_{i,j}) \mapsto (\epsilon_j y_{i,j+1})$. Since each v_i is sent to $-v_i$ by σ, $v_{i,j+1} = -\epsilon_j v_{i,j}$, or $v_{i,j}v_{i,j+1} = \epsilon_j$. Hence

$$\sum_{i=1}^{s} \sum_{j=1}^{r/2} v_{i,j}v_{i,j+1}x_{i,j}y_{i,j+1} = \sum_{i=1}^{s} \sum_{j=1}^{r/2} \epsilon_j x_{i,j}y_{i,j+1}$$

But $\epsilon_j x_{i,j} = (\sigma x)_{i,j+1}$. Therefore

$$\sum_{i=1}^{s} \sum_{j=1}^{r/2} \epsilon_j x_{i,j}y_{i,j+1} = \sum_{i=1}^{s} \sum_{j=1}^{r/2} (\sigma x)_{i,j+1}y_{i,j+1} = 0.$$

Each of the other sums is in a similar manner seen to be 0 - Q.E.D.

REMARK. The situation is even simpler over GF(2). For example, the extended Hamming (8, 4) code under χ: $i \mapsto -i^{-1}$ (mod 7) whose orbits are $(0, \infty)(1, 6)(2, 3)(4, 5)$ is mapped onto the obvious (4, 2) self-orthogonal code.

3. The (60, 30) QR Code Over GF(3).

We now choose A to be a (60, 30) extended quadratic residue code over GF(3). $PSL_2(59)$ has order 60.59.29, and from Dickson [3] (or Sylow) we know that in particular there are elements of order 5 in $PSL_2(59)$. We actually compute an invariance σ of the code A which has its permutation part of order 5 and which satisfies $\sigma^5 = -1$. (The computation is sketched in the Appendix.)

We then get 12 vectors $v_1, \ldots, v_{12}$ each of weight 5, such that $\sigma(v_i) = -v_i$ for $i = 1, \ldots, 12$. Using these, we map A to a subspace of $GF(3)^{12}$ which, by our previous Theorem, is orthogonal to itself. We calculated that in fact it has dimension 6, and we then proved it was equivalent to the Golay (12, 6) code by the following method.

We chose six linearly independent vectors from $\psi(A)$ and by row operations and column interchanges obtained the following six vectors (+ = 1, - = - 1, blank = 0):

$$\begin{array}{cccccccccccc}
1 & 2 & 3 & 4 & 5 & 6 & 7 & 8 & 9 & 10 & 11 & 12 \\
+ & & & & & & - & 0 & + & + & - & - \\
 & + & & & & & - & - & + & - & + & 0 \\
 & & - & & & & + & - & + & + & 0 & + \\
 & & & & - & & - & - & - & 0 & - & + \\
 & & & - & & & - & + & 0 & + & + & + \\
 & & & & & + & 0 & + & + & - & - & +
\end{array}$$

Then by monomial operations we transformed the right-hand half of this array into

$$\begin{array}{cccccc}
0 & + & + & + & + & + \\
+ & 0 & + & - & - & + \\
+ & + & 0 & + & - & - \\
+ & - & + & 0 & + & - \\
+ & - & - & + & 0 & + \\
+ & + & - & - & + & 0
\end{array}$$

which is Pless's matrix S_5 in her generation of the Golay (12, 6) code by $(I_6; S_5)$ [5]. Therefore we have proved

PROPOSITION 1. When A is the (60, 30) extended quadratic residue code over GF(3) and σ is any non-trivial invariance of A such that $\sigma^5 = -1$, then the mapping ψ defined previously maps A onto the Golay (12, 6) code over GF(3).

Proof. We proved this for one such σ, but all are conjugate in the invariance group of A.

COROLLARY. No vector v of weight 15 in A can be stabilized by an invariance σ of the type described in Proposition 1 (stabilizing is taken in the sense that $\sigma v = -v$).

This is true because v would have to be $v_i \pm v_j \pm v_k$ for three of the special $v_1, \ldots, v_{12}$. But then ψ would map v to a vector of weight 3, and there are none in the Golay code.

PROPOSITION 2. If m = 0 in (2), then n = 0 also. That is, if A has no weight 12 vectors, it has no weight 15 vectors, either.

Proof. If m = 0, then n is the number of weight 15 vectors in A. Thus $n \geq 0$. The invariance group of the code, "2 $PSL_2(59)$," has order $60 \cdot 59 \cdot 58 = 3 \cdot 68,440$. Since the number of weight 60 vectors in A is 41, 184 - n, n must be less than 41, 184. By [1, p. 148] the stabilizer (permutationally) of a weight 15 must have order dividing 15, i.e., the order must be 1, 3, 5, or 15. It cannot be 5 or 15 by the Corollary above. But if it is 1 or 3, there are at least 68, 440 vectors of weight 15, a contradiction - Q.E.D.

Thus we have reduced the question of the minimum distance in the (60, 30) quadratic residue code over GF(3) to the question of the existence of weight 12 vectors in the code. For this question, we now develop a computationally feasible approach. It is based on Pless' s method [5] for her symmetry codes over GF(3).

4. On the Minimum Weight in Cyclic Codes.

Let n = 2k + 1 be an odd integer and let A be a cyclic (n, k) code over F = GF(q). Pick a generating matrix for the code as follows:

$$G = [I_k; C; S]$$

where I_k is the $k \times k$ identity matrix, C is a $k \times 1$ matrix, and S a $k \times k$ matrix. Suppose one knows that A has a minimum weight $\geq w$, where w is an even integer. (The case of w odd is easily treated also, but we do not do this here.) We describe a method for determining whether or not the minimum weight is w. In fact, we prove the following.

THEOREM 2. If every vector of A with weight $\leq w/2 - 1$ on the first k coordinates has weight $> w$, then A has minimum weight $> w$.

Proof. Let $a \in A$ have weight $\leq w$. Then the weight of a on the first k coordinates must be $\geq w/2$, by assumption. We can insure, by cycling to the left if necessary, that a has a non-zero entry on the $(k + 1)$-st coordinate. This having been done, the cycled a still must have weight $\geq w/2$ on the first k coordinates by assumption, since cycling does not change the weight. On the last k coordinates, a now has weight $\leq w/2 - 1$. But by cycling k times to the right, the new a will have weight $\leq w/2 - 1$ on the first k coordinates, a contradiction. Hence the Theorem.

Thus, the total number of code-vectors to be examined is at most

$$\sum_{i=0}^{w/2-1} \binom{k}{i}(q - 1)^{i-1}$$

In examining code-vectors in accordance with Theorem 2, one easily sees that if the coordinate is 0 in the position designated C on page IV-7, then a cycle of that vector once to the left will produce a vector already examined (if we run through the subsets lexicographically from the left - as we did; i.e., the first 5-subset of rows was $\{0, 1, 2, 3, 4\}$, the next was $\{0, 1, 2, 3, 5\}$, and the last was $\{24, 25, 26, 27, 28\}$. Such a vector need not be further processed.) Implementing this observation reduced the computer time needed by about 1/3.

Note that for the (60, 30) extended quadratic residue code over GF(3) we know that $d \geq 12$; and we can examine the cyclic (59, 29) "small" quadratic residue code (of the same minimum weight as the (60, 30)). Thus at most

$$\sum_{i=0}^{5} \binom{29}{i} \cdot 2^{i-1} = 2,105,545$$

vectors need be examined.

The above procedure was carried out by means of a Fortran program on a PDP-10 time-sharing system. Internal checks were made to see whether each vector calculated had weight divisible by 3 and to print the total number of code-vectors calculated. Both these checks were satisfactory. Another check was an instruction to print any vector with weight less than 18. This was never executed. Therefore, we conclude that the (60, 30) extended quadratic residue code over GF(3) has minimum distance 18, and that therefore, by [1], the code-vectors of weight w, for $18 \leq w \leq 33$, yield 5-designs. These 5-designs have, of course, the same parameters as those arising from the Pless codes [5]; but as Pless has shown, hers and ours are inequivalent, because they have different automorphism groups: Pless has shown that the group acting on her designs contains $PSL_2(29)$; this cannot be contained in the automorphism group of the present designs, which is $PSL_2(59)$.

We are grateful to David J. Segal for assistance in programming this problem.

5. Appendix.

Using the isomophism between $SL_2(59)$ and the matrix group over $GF(59^2)$ consisting of all matrices of the form

$$\begin{pmatrix} a & b \\ -b^{59} & a^{59} \end{pmatrix}$$

with determinant 1 (Dickson [3] page 264), we calculated a 60th root θ of 1 in $GF(59^2)$: the matrix $\begin{pmatrix} \theta & 0 \\ 0 & \theta^{-1} \end{pmatrix}$ then corresponds to what we want in $SL_2(59)$.

Let $\theta \epsilon\ GF(\ell^2)$ be such that $\theta^{\ell+1} = 1$, a primitive $(\ell + 1)$-st root of unity. Then $\begin{pmatrix} \theta & 0 \\ 0 & \theta^{-1} \end{pmatrix}$ has order $(\ell + 1)/2$ when viewed in $SL_2(GF(\ell^2))$. Set $J = \begin{pmatrix} \rho & 1 \\ \rho\theta^{\ell} & \theta \end{pmatrix}$, where $\rho^{\ell+1} = -1$. Then

$$J \begin{pmatrix} \theta & 0 \\ 0 & \theta^{-1} \end{pmatrix} J^{-1} = \begin{pmatrix} \theta + \theta^{\ell} & -1 \\ 1 & 0 \end{pmatrix}$$

is of order $(\ell + 1)/2$ when viewed in $SL_2(\ell)$. $\theta + \theta^{\ell}$ is the trace of θ from $GF(\ell^2)$ to $GF(\ell)$, so the desired element of $SL_2(\ell)$ is that on the right.

The calculation of θ proceeds: let $K = GF(59^2)$ and $F = GF(59)$. Then K consists of all roots of 1 of order dividing $60 \cdot 58$. Aside from ±1, the 60th roots of 1 in K are therefore all the roots of all the irreducible second-degree polynomials over F, since these are the elements of K not in F. Such polynomials have the form

$$f_a(x) = x^2 - ax + 1,$$

since the constant term must be $\alpha \cdot \alpha^{59} = \alpha^{60} = 1$. They are reducible if and only if $a^2 - 4$ is 0 or a quadratic residue mod 59. Since $2^2 - 4 = 0$, $3^2 - 4 = 5$, $4^2 - 4 = 12$, $5^2 - 4 = 21$, $f_a(x)$ is reducible for $\pm a = 1, \ldots, 5$; but it is irreducible for $a = \pm 6$. We then found

$$x^{12} \equiv -x^2 \pmod{x^2 - 6x + 1},$$

which means $f_6(x)$ has exponent 20, and that roots of it are therefore primitive roots of 1 of order 20. We denote a root of $x^2 - 6x + 1$ by x and take 1 and x as a vector-space basis for

K over F. We put $w = cx + d$ and solve for c and d in F in the equation $w^2 + w + 1 = 0$, making w a primitive cube root of 1. Then $\theta = wx$ is a primitive 60^{th} root of 1, and $\theta = 10(3x - 2)$. Thus trace $\theta = 10(3 \cdot 6 - 2 \cdot 2) = 22$. Hence

$$\begin{pmatrix} 22 & -1 \\ 1 & 0 \end{pmatrix}$$

or the permutation $y \mapsto 22 - y^{-1}$ of $\{GF(59) \cup \infty\}$, is what we want.

We find the signs for the monomial representation of this invariance by the factorization

$$\begin{pmatrix} 22 & -1 \\ 1 & 0 \end{pmatrix} = \begin{pmatrix} 1 & 22 \\ 0 & 1 \end{pmatrix} \begin{pmatrix} 0 & -1 \\ 1 & 0 \end{pmatrix}$$

The first of these is the cyclic shift raised to the 22nd power; the other is the special involution of $PSL_2(59)$, the signs for which are given in [1, p. 131]. Thus our monomial raised to the 6^{th} power is given by the following array:

Monomial Transformation					"Fixed" Vector				
58	16-	31-	40-	48	+	+	+	+	-
23-	33	41	50-	6-	+	-	+	+	+
4-	47	45-	9	12-	+	-	-	+	+
7-	27-	1	35	17-	+	+	-	+	+
5-	46-	21	54	15-	+	+	-	+	+
10-	13-	36	34-	18	+	+	-	-	+
22	57	14	26	28-	+	-	+	-	-
30	52	43-	56-	3-	+	-	-	-	-
20-	39	11-	42-	2	+	-	-	-	+
51	19	25-	38-	29-	-	+	+	+	+
0	53	55-	8	24	+	-	-	+	-
∞-	32	37	44	49	-	+	-	+	-

Read across a row from left to right to see the permutation action of the order-5 element; read down a column to see the action of the element of order 30. The signs are interpreted as follows: for row 1, the permutation matrix corresponding to (58, 16, 31, 40, 48) is made by row permutations of the identity matrix. Then the indicated rows are multiplied by minus signs (rows 16, 31 and 40). In other words, the coordinate value in place 58 goes to place 16 and is multiplied by -1. These signs are not so interpretable for the element of order 30.

References

[1] E.F. Assmus, Jr., and H.F. Mattson, Jr., "New 5-Designs," J. Combinatorial Theory 6 (1969), pp. 122-151 (plus Addendum dated 30 June 1969).

[2] A.M. Gleason, "Weight Distributions of Formally Self-Orthogonal Codes," Private Communication, August 1969.

[3] L.E. Dickson, Linear Groups, Dover, N.Y., 1958.

[4] John N. Pierce, "Weight-Distribution of the Ternary (60, 30) Self-Orthogonal Code with Minimum Distance 18," Private Communication, August 21, 1969.

[5] Vera S. Pless, "On a New Family of Symmetry Codes Over GF(3) and Related New 5-Designs," J. Combinatorial Theory (to appear).

PART V

MISCELLANEOUS RESULTS

SECTION 1

A REMARK ON PERFECT BINARY CODES

PROPOSITION. Let $A \subseteq GF(2)^n$ be a linear perfect code with $d = 2e + 1$ and $e \geq 1$. Then, not only does $e + 1$ divide $n - e$ but $(n - e)/(e + 1)$ is odd and A contains the all-1 vector. Moreover, λ_h (defined below) is odd for $h = 0, 1, \ldots, e$.

Proof. That $e + 1$ divides $n - e$ follows from design considerations (see for example [1], p. 250). There are $(n - e)/(e + 1)$ code-vectors of weight d with 1's at e given places and necessarily having no more common 1's. The existence of these vectors comes from design considerations - see [1]. If $(n - e)/(e + 1)$ is even, then the sum of all these vectors is a vector of weight $n - e$; and every vector of weight $n - e$ is in A. This is obviously impossible. Hence $(n - e)/(e + 1)$ is odd and the sum is the all-1 vector.

The basic idea here is to use the characterizing property of perfect binary codes, that the minimum-weight vectors form a tactical configuration of type 1; $(e + 1) - d - n$. Then these vectors also form tactical configurations of type

$$\lambda_h = \frac{\binom{n-h}{e+1-h}}{\binom{d-h}{e+1-h}}; h - d - n, \text{ for } h = 0^*, 1, \ldots, e$$

Thus, for $h = e$, we get the result of the previous paragraph; for $h = e - 1$ we have

$$\lambda_{e-1} = \frac{n - e + 1}{e + 2} \cdot \frac{n - e}{e + 1}$$

and if we consider the λ_{e-1} code-vectors of weight d covering a given $e - 1$ places, we see that each coordinate position outside the chosen $(e - 1)$-set is covered by exactly λ_e of these vectors. Thus, since λ_e is odd, if we add all these vectors we get all 1's outside the chosen $(e - 1)$-set, and by the same argument as in the previous case, we conclude that λ_{e-1} is odd. Since

$$\lambda_{e-1} = \frac{n - e + 1}{e + 2} \lambda_e$$

*λ_0 is the number of minimum-weight vectors.

it follows that n - e + 1 and e + 2 are exactly divisible by the same power of 2. The same conclusion holds for n - e + 2 and e + 3, for n - e + 3 and e + 4, ..., and for n and 2e + 1.

References

[1] E.F. Assmus, Jr., and H.F. Mattson, Jr., "Tactical Configurations and Error-Correcting Codes," J. Comb. Theory, 2 (1967), pp. 243-257, MR 36, #64.

PART V

SECTION 2

ON A PROBLEM OF SEIDEL

We found the Proposition of this section in response to a question of J. J. Seidel. It is related to the question whether his "1288" graph [2] is strongly regular.

1. Definition of the Graph.

The Golay code consists of 4,096 vectors of 24 coordinates over 0, 1. Aside from the all-0 and all-1 vectors, it consists of 759 vectors of weight 8, 2576 of weight 12, and 759 of weight 16. Since the code is self-orthogonal under the usual inner product, any two code-vectors must have an even number of 1's in common positions with each other. It is well known that the Mathieu group M_{24} is the automorphism group of the code.

The vertices of the graph are the code-vectors of weight 12. Two vertices are joined by an edge if and only if they have exactly 6 common 1's.

2. The Action of M_{24}.

Let us call the code-vectors of weights 8 and 12 8-clubs and 12-clubs. An 8-club and a 12-club meet in 0, 2, 4, or 6 points. Then there are 2576 12-clubs, and it happens that (order of M_{24}) ÷ (order of M_{12}) = 2576. The stabilizer of a 12-club must therefore have order at least that of M_{12}.

But inside a given 12-club there is a 5-6-12 Steiner system selected uniquely by the code; i.e., we choose for each 5-set of coordinates in the 12-club the unique 8-club of the code containing it; this 8-club must intersect the 12-club in 6 points, which make the 6-club of the Steiner system we seek. Since now the stabilizer of the 12-club permutes all the 8-clubs, it is a group of automorphisms of the 5-6-12 Steiner system and hence has order at most that of M_{12}. Therefore, M_{12} is the stabilizer of a 12-club, and M_{24} is transitive on the 12-clubs. In particular, we see that the graph is regular.

The 6-clubs of the 5-6-12 Steiner system are 132 in number, and the other 6-subsets of the 12 points are 792 in number. These latter are the sets of intersection of two 12-clubs meeting in six points, for such 6 points cannot be contained in an 8-club since the sum of the two 12-clubs and the 8-club would be a code-vector of weight 20; and M_{12} is transitive on the 132 6-clubs and on the 792 other 6-sets.

Now consider the graph defined above. By the transitivity of M_{24} on the 12-clubs and of M_{12} on the "non-club" 6-sets, any vertex and emanating edge may be taken to a preassigned vertex and to a preassigned non-club 6-set within it. The latter, however, gives rise to two edges for the other two 12-clubs meeting the preassigned one in exactly those six points. Thus we have started with vertices X and Y joined by an edge, and have mapped X to A and Y to B or C in the triangle ABC. In ABC the underlying 6-set S of intersection is the same for every edge. Now, Todd [1] displays an element t of order 3 in M_{24} which fixes S pointwise and is transitive in A. B. C. Thus, if (X, Y) goes to (A, B) we can operate with t to send B to A and A to C, sending (X, Y) to (C, A). Thus

PROPOSITION. M_{24} is edge-transitive on the graph.

The valence of this graph is 2,792.

Seidel's actual concern is with his "1288" graph, obtained from the above graph by identifying the vertex A with its complement A', and four edges joining them to B, B' (if one edge exists, all exist).

References

[1] J.A. Todd, "A Representation of the Mathieu Group M_{24} as a Collineation Group," Annali di Mathematica Pura ed Applicata, (IV) Vol. LXXI (1966), pp. 199-238.

[2] J.M. Goethals and J.J. Seidel, "Strongly Regular Graphs Derived from Combinational Designs," Canadian J. Math. XXII (1970), pp. 597-614.

PART V

SECTION 3

A CLASS OF (16k, 7k + 1) CODES FOR k ODD

Let A be an (8, 4) extended Hamming code, B its reverse. Thus, $A \cap B = \{0, \text{all-1}\}$, A + B = all even-weight vectors. Now set

$$V = \underbrace{(A; A; \dots ; A)}_{k\text{-times}};\underbrace{(B; B; \dots ; B)}_{k\text{-times}},$$

where the semicolon ";" denotes juxtaposition of codes (external direct sum). Map V into $GF(2)^{16k}$ via

$$(a_1, \dots, a_k; b_1, \dots, b_k) \mapsto (a_1 + \sum_{i \neq 1} b_i,\ a_2 + \sum_{i \neq 2} b_i,\ \dots ;\ b_1 + \sum_{i \neq 1} a_i;$$

$$b_2 + \sum_{i \neq 2} a_i,\ \dots).$$

Clearly, dim V = 8k. We show that the kernel has dimension k - 1 and hence C = image of V in $GF(2)^{16k}$ has dimensions 8k - (k - 1) = 7k + 1.

If $a_j + \sum_{i \neq j} b_i = (00 \dots 0)$, then either $a_j = 0$ and $\sum_{i \neq j} b_i = 0$ or $a_j = \text{all-1}$ and $\sum_{i \neq j} b_i = \text{all-1}$. Assume we have a representation of $0 \epsilon C$ with $a_1 = a_2 = \dots = a_r = \text{all-1}$ and $a_{r+1} \dots = a_k = 0$. Let d(C) denote the minimum weight in C.

<u>Case</u> 1. r odd. Then it follows that $b_{r+1} = b_{r+2} = \dots = b_k = \text{all-1}$ and $b_1 = b_2 = \dots = b_r = 0$. Since k is odd, k - r is even and hence $a_1 = 0$ - a contradiction.

<u>Case 2</u>. r even. Then $b_1 = b_2 = \dots = b_r = \text{all-1}$ and $b_{r+1} = \dots = b_k = \text{all-1}$. Now k - r is odd and we have a representation of 0. Thus, there are $\binom{k}{0} + \binom{k}{2} + \dots + \binom{k}{k-1} = (1/2)\ 2^k = 2^{k-1}$ elements in the kernel and this proves our assertion.

For k = 1, C = A; B. For $k \geqq 3$, $d(C) \leqq 8$ since we can take $a_1 = 11010001$, $b_1 = 11000101$, $a_3 = b_3 = \text{all-1}$ and $a_2 = a_3 + a_1$, $b_2 = b_3 + b_1$. Then we get $(a_1 + b_1, a_2 + b_2, 0, \dots 0; a_1 + b_1, a_2 + b_2, 0, \dots, 0)$ which has weight 8. (Here $a_i = b_i = 0$ for $i > 3$.)

One checks easily that C is contained in its orthogonal. Since C has a generating set consisting of vectors whose weights are $\equiv 0 \pmod 4$, C has all weights $\equiv 0 \pmod 4$.

Summary. For each odd k we have constructed a $(16k, 7k+1)$ binary code C contained in its own orthogonal, having all weights divisible by 4, and containing vectors of weight 8.

PART V

SECTION 4

THE TWO SELF-ORTHOGONAL (16, 8) CODES OVER GF(2) WHOSE WEIGHTS ARE DIVISIBLE BY 4

The unique weight distribution for a code of the title is, by the MacWilliams equations,

0	4	8	12	16
1	28	198	28	1

One such code, A, is the direct sum of two extended Hamming codes, (8, 4). Another, B, is given by the row space of the following matrix, M:

$$\begin{matrix}
11 & 11 & 00 & 00 & 00 & 00 & 00 & 00 \\
11 & 00 & 11 & 00 & 00 & 00 & 00 & 00 \\
11 & 00 & 00 & 11 & 00 & 00 & 00 & 00 \\
\cdot & & & & & & & \\
\cdot & & & & & & & \\
\cdot & & & & & & & \\
11 & 00 & 00 & 00 & 00 & 00 & 00 & 11 \\
10 & 10 & 10 & 10 & 10 & 10 & 10 & 10
\end{matrix}$$

These two codes are obviously inequivalent because seven weight 4 vectors of A never appear in the configuration shown in the matrix M.

We now show that any (16, 8) self-orthogonal code over GF(2) all of whose weights are divisible by four is equivalent to either A or B. Suppose C is such a code. Theorem 4.2 of [1] shows that the vectors of each weight class form a 1-design. Hence, given any coordinate of C, there are seven weight 4 vectors with a 1 at that coordinate.

Suppose first they can be brought to the form of the first seven rows of the matrix M; i.e., that they all share another coordinate where they are 1. The 7-dimensional space they generate contains $\binom{7}{3} + \binom{7}{4} = 70$ weight 8 vectors. Hence there are in C 128 further weight 8 vectors. Any one of these must have precisely one 1 in each of the eight blocks of two displayed in the matrix M, for if it had two 1's in any block of two it would have to have either no 1's or two 1's in every other block and it would have already been

PART V

SECTION 5

A RESULT ON THE AUTOMORPHISM GROUP OF A 4-DESIGN CODE

Let A be an (n, k) code over a finite field F with $d(A) \geq 4$. Suppose the minimum weight vectors yield a 4-design with λ_2, λ_3, λ_4 satisfying

$$\lambda_2 - 2\lambda_3 + \lambda_4 > 0$$

$$\lambda_2 \neq \lambda_1$$

(conditions which are "always" satisfied). Then we claim that the invariance group of A cannot contain a transposition.

To prove this claim, suppose (12)(3)(4) ... (n) is in the invariance group, i.e., there is an invariance acting by the rule $(a_1, a_2, \ldots, a_n)\,\sigma =$

$$(\alpha_2 a_2, \alpha_1 a_1, \alpha_3 a_3, \ldots, \alpha_n a_n)$$

The minimum weight vectors with $a_1 = a_2 = 0$ yield a 2-design on $\{3, 4, \ldots, n\}$ whose λ is $\lambda_2 - 2\lambda_3 + \lambda_4$.[*] This implies that $\alpha_3 = \alpha_4 = \ldots = \alpha_n$ for otherwise $a - a\sigma$ has weight less than 4 for some minimum weight a with $a_1 = a_2 = 0$. So we can assume $\alpha_3 = \alpha_4 = \ldots = \alpha_n = 1$. Since $\lambda_2 \neq \lambda_1$, we choose a minimal weight a with $a_1 = 0$, $a_2 \neq 0$. Then $a - a\sigma$ has weight 2 - a contradiction.

[*] That is, every pair among 3, 4, ..., n is covered by λ_2 minimum weight vectors, of which $2\lambda_3 - \lambda_4$ cover one or two of the spots 1, 2.

PART V

SECTION 6

ON LINEAR CODES SUPPORTED BY STEINER TRIPLE SYSTEMS

1. Introduction.

Peyton Young conjectured to us at the Chapel Hill Conference in May, 1970 that there are several t-designs for large t, in particular that there is a 1;9-10-20 design. If so, then the contraction of that design is a Steiner triple system on 13 points. If the design on 20 points arises as the support of all the vectors of weight 10 in some linear code, then the analogue holds for the weight 3 vectors in the contracted code of length 13. These considerations motivated our attempt to determine whether Steiner triple systems (hereinafter called STS) can support codes. We record some results which may be helpful in performing the necessarily tedious calculations involved in this question.

An old and related result will serve as an example. There is a unique Steiner system of type 1;3-5-17 (see [2], Satz 6) and it has the parameters to support a perfect binary code, namely, 1;(e + 1) - d - n. But no such code exists. Therefore, this Steiner system does not support any binary code.

A simpler example is the STS on seven points; it supports the well known Hamming (7, 4) binary code.

The perfect (11, 6) ternary code of Golay has minimum distance 5. Thus, the contraction of it to length 9 yields a code supported by the STS on nine points.

2. Calculations.

We consider a STS on the set S of n points. It is well known that $n \equiv 1$ or 3 (mod 6) and that the number of triples is $n(n - 1)/6$.

Suppose A is a code over GF(q) of which the minimum weight vectors "are" the triples of the STS. Since $d \leq n - k + 1$ and the code is not optimal, we have $k < n - 2$.

Let Y be an m-subset of S, $m \geq 3$, and y_i the number of triples which meet Y in exactly i spots; then one can easily verify that

$$\sum_{i=s}^{m} \binom{i}{s} y_i = \lambda_s \binom{m}{s} \qquad s = 0,\ 1,\ 2,$$

where λ_0 is the total number of triples, λ_1 is the number of triples covering one point, $\lambda_1 = (n - 1)/2$, and $\lambda_2 = 1$. In our case the equations are

$$y_0 + y_1 + y_2 + y_3 = n\,(n - 1)/6$$

$$y_1 + 2y_2 + 3y_3 = (n - 1)m/2$$

$$y_2 + 3y_3 = m(m - 1)/2 \qquad (1)$$

From now on, we take Y to be the support of a vector of weight m in the orthogonal code $A^{\perp}$. Then y_1 must be 0, and (1) becomes

$$y_0 = \frac{1}{6}\,(n - m)(n - m - 1)$$

$$y_2 = m\,(n - m)/2$$

$$y_3 = m\,(2m - n - 1)/6 \qquad (2)$$

We assume $y_0 > 0$, and then the value of y_0 in (2) implies that the triples contained in the complement of Y form a Steiner triple system on n - m points, hence $m \leq n - 3$.

The value for y_3 implies

$$m \geq \frac{n + 1}{2},$$

and

$$m(2m - n - 1) = 0 \pmod 6 \qquad (3)$$

Since $n \equiv 1,\ 3 \pmod 6$ and $n - m \equiv 1,\ 3 \pmod 6$ we consider cases:

Case $n \equiv 1 \pmod 6$:

$$m(2m - 2) \equiv 0\ (6)$$
$$1 - m \equiv 1,\ 3\ (6)$$

or

$$m(m - 1) \equiv 0\ (3)$$

$$m \equiv 0,\ 4\ (6) \qquad (4)$$

And $m \equiv 0,\ 4 \pmod 6$ implies that $m \equiv 0,\ 1 \pmod 3$.

Conclusion: if m is not n or n - 1, then $n \equiv 1 \pmod 6$ implies $m \equiv 0,\ 4 \pmod 6$.

Case $n = 3 \pmod 6$:

$$m(2m - 4) \equiv 0 \ (6)$$
$$3 - m \equiv 1 \text{ or } 3 \ (6)$$

The second implies the first.

Conclusion: If m is not n or n - 1, then $n \equiv 3 \pmod 6$ implies $m \equiv 0, 2 \pmod 6$.

We now rewrite y_3 as

$$y_3 = \frac{m(m - 1)}{6} - \frac{m(n - m)}{6} \qquad (6)$$

and note that the number of 2-subsets of Y covered by the y_3 triples of the system contained in Y is

$$3y_3 = \binom{m}{2} + \frac{m(m - n)}{2}$$

Notice that the values $m = n, n - 1, n - 2$ are settled in that n and n - 1 are possible weights in an orthogonal code; but n - 2 is never possible, since such a vector could not annihilate the triple covering its two 0-positions. Thus we treat the case $m \leq n - 3$.

We now look at the MacWilliams equations. Assume that the minimum weight in $A^\perp$ is n - 3, which holds, for example, if the STS has no subsystems since if there were in $A^\perp$ a vector v of weight less than n - 3, every triple covering two of the 0's of v would have its third point also on one of the 0's of v. Thus, triples "on" the 0's of v would constitute a subsystem. (We ignore the trivial STS on three points at the moment.)

REMARK 1. $A^\perp$ has dimension 3 because it is not optimal and thus

$$n - (n - k) + 1 \geq n - 3$$

or $n - k < 4$. We already know $k < n - 2$; hence $k = n - 3$ and $n - k = 3$.

The equations are [1] ($A^\perp$ has weight distribution $\{B_i\}$)

$$B_{n-3} + B_{n-1} + B_n = q^3 - 1$$

$$3B_{n-3} + B_{n-1} = \sum_{\nu=0}^{1} (n)_\nu q^{3-\nu} S(1, \nu) - n$$

$$3^2 B_{n-3} + B_{n-1} = \sum_{\nu=0}^{2} (n)\nu q^{3-\nu} S(2, \nu) - n^2 \qquad (7)$$

Since $x^r = \Sigma S(r, \nu)(x)_\nu$, S(1, 0) = S(2, 0) = 0 and S(1, 1) = S(2, 1) = S(2, 2) = 1. Thus

$$B_{n-3} + B_{n-1} + B_n = q^3 - 1$$

$$3B_{n-3} + B_{n-1} = nq^2 - n$$

$$3^2 B_{n-3} + B_{n-1} = nq^2 + n(n - 1)q - n^2 \qquad (8)$$

These have the unique solution

$$6B_{n-3} = n(n - 1)(q - 1)$$

$$B_{n-3} = n(n - 1)(q - 1)/6$$

$$B_{n-1} = n(q^2 - 1) - n(n - 1)(q - 1)/2$$

$$= n(q - 1)(q + 1 - (n - 1)/2) \qquad (9)$$

which implies in particular

$$q \geq \frac{n - 3}{2}. \qquad (10)$$

From (8) and (9) we then find

$$B_n = q^3 - 1 - n(q - 1)\left[q - \frac{n - 3}{2} + \frac{n - 1}{6}\right]$$

or

$$B_n = q^3 - 1 - n(q - 1)\left[q - \frac{n - 4}{3}\right] \qquad (11)$$

We factor q - 1 out of (11) and regard what remains as a quadratic in q; it has discriminant (n - 1) · (9 - n)/3. This means B_n is positive for n ≥ 9. And, in general, we have

$$\frac{B_n}{q - 1} = \left(q - \frac{n - 1}{2}\right)^2 - \frac{(n - 1)(9 - n)}{12}$$

Since we care only about n ≡ 1 or 3 (mod 6), we treat only n = 7 here (the cases n = 1 or 3 being too trivial to bother with). Then $B_7/(q - 1) = (q - 3)^2 - 1$, which is 0 for q = 2 or 4, -1 for q = 3, and positive for q ≥ 5. In particular, then, we have shown that on suitable change of scalars, the all-1 vector is in the orthogonal of every code supporting a STS except that on 7 points for q = 2 or q = 4; and we have shown that there is no code supporting the 7-point STS over GF(3).

A Check for Consistency. Equations (8) and (9) imply, from the MacWilliams relations, that the number of weight 3 and 4 vectors in A is:

$$A_3 = \frac{n(n-1)}{6}(q-1)$$

$$A_4 = \frac{n(n-1)}{24}(q-1)(n-6)(n-3) \qquad (12)$$

If the design comes from a larger design, there should be $n(n-1)(q-1)\left(\frac{n+1}{24} - \frac{1}{6}\right)$ 4-sets present from the code, but there are many more. This difference is caused by the fact that the weight 4's in the code don't form a design since two weight 4's can occupy the same places without being scalar multiples of each other.

For the record we set down our finding that

$$A_5 = \frac{n(n-1)(q-1)}{120}\left[q(n-2)(n-3)(n-4) + n^3 + 36n^2 - 104n + 96\right].$$

References

[1] Vera S. Pless, "Power Moment Identities on Weight Distributions in Error-Correcting Codes," Inf. and Control, 6 (1963), pp. 147-152.

[2] E. Witt, "Über Steinersche Systeme," Abh. Math. Sem. Hansischen Univ., 12 (1936), pp. 265-275.

PART V

SECTION 7

TWO SMALL REMARKS ON PACKING

The alternating group Alt(n) is evidently a distance-3 packing of n-space over n symbols with no symbols repeated in a word. The cardinality of the packing set is n!/2.

If n = q is a prime power, then we can define the Reed-Solomon code on n symbols with $3 = d = n - k + 1$ or $k = n - 2$. This code has cardinality $q^{n-2} = n^{n-2}$, which is larger than n!/2 if $n \geq 4$.

DOCUMENT CONTROL DATA - R & D

(Security classification of title, body of abstract and indexing annotation must be entered when the overall report is classified)

1. ORIGINATING ACTIVITY *(Corporate author)*

Sylvania Electronic Systems Eastern Division
An Operating Group of Sylvania Electric Products Inc.
77 A Street, Needham Heights, Massachusetts 02194

2a. REPORT SECURITY CLASSIFICATION
Unclassified

2b. GROUP
None

3. REPORT TITLE

ALGEBRAIC THEORY OF CODES II

4. DESCRIPTIVE NOTES *(Type of report and inclusive dates)*
Scientific. Final: (16 September 1969 to 15 September 1970) Approved: 15 January 1971

5. AUTHOR(S) *(First name, middle initial, last name)*

Edward F. Assmus, Jr.
Harold F. Mattson, Jr.

6. REPORT DATE
15 October 1970

7a. TOTAL NO OF PAGES
65

7b. NO. OF REFS
25

8a. CONTRACT OR GRANT NO
F19628-69-C-0068

b. PROJECT, Task, Work Unit Nos.
5~~8~~628-01-01

c. DoD Element 61102F

d. DoD Subelement 681305

9a. ORIGINATOR'S REPORT NUMBER(S)
FR70-3N

9b. OTHER REPORT NO(S) *(Any other numbers that may be assigned this report)*
AFCRL-71-0013

10 DISTRIBUTION STATEMENT

1- This document has been approved for public release and sale; its distribution is unlimited.

11. SUPPLEMENTARY NOTES
TECH, OTHER

12. SPONSORING MILITARY ACTIVITY
Air Force Cambridge Research Laboratories (LR)
L. G. Hanscom Field
Bedford, Massachusetts 01730

13. ABSTRACT

The resultant is applied to the problem of weights in cyclic codes. The binary code arising from the projective plane of order 10 (if it exists) is examined. T-design decoding is discussed in general, and the special case of the (48, 24) binary extended quadratic residue code is worked out in detail. The (60, 30) ternary extended quadratic residue code is proved to yield new 5-designs. Miscellaneous results include study of the question whether Steiner triple systems support linear codes.

14. KEY WORDS	LINK A		LINK B		LINK C	
	ROLE	WT	ROLE	WT	ROLE	WT
Cyclic codes						
Weights						
Majority logic decoding						
Resultant						
Projective plane						
5-design						
Quadratic residue codes						
Steiner triple systems						
Perfect binary codes						
Golay code; graph						
(16, 8) binary codes						
Packing						

ERRATA

FINAL REPORT

ALGEBRAIC THEORY OF CODES II

AFCRL-71-0013

On the cover and title page of the above technical report, change the following:

	From	To
Project No.	5628	8628
Task No.	562801	862801
Work Unit No.	56280101	86280101

Errata prepared per directions
Air Force Cambridge Research Laboratories, AFSC,
USAF, Bedford, Mass. 01730

Contract No. F19628-69-C-0068

GTE SYLVANIA
INCORPORATED
ELECTRONIC SYSTEMS GROUP
EASTERN DIVISION

77 "A" STREET
NEEDHAM HEIGHTS, MASSACHUSETTS 02194

END

DATE

FILMED

6-17-71